# MISSISSIPPI LAW JOURNAL

## SYMPOSIUM

## THE SEARCH AND SEIZURE OF COMPUTERS AND ELECTRONIC EVIDENCE

**Sponsored by the**
**National Center for Justice**
**and the Rule of Law**

THE FOURTH AMENDMENT IN AN ERA OF UBIQUITOUS TECHNOLOGY
*Susan W. Brenner*

SEARCH WARRANTS IN AN ERA OF DIGITAL EVIDENCE
*Orin S. Kerr*

TRANSACTION SURVEILLANCE BY THE GOVERNMENT
*Christopher Slobogin*

THE FOURTH AMENDMENT ASPECTS OF COMPUTER SEARCHES AND SEIZURES: A PERSPECTIVE AND A PRIMER
*Thomas K. Clancy*

COMPUTER SEARCHES OF PROBATIONERS—DIMINISHED PRIVACIES, "SPECIAL NEEDS" & "'*WHILST' QUIET* PEDOPHILES"—PLUGGING THE FOURTH AMENDMENT INTO THE "VIRTUAL HOME VISIT"
*Marc M. Harrold*

**VOLUME 75** **FALL 2005** **NUMBER 1**

RECENT DECISIONS
OF THE MISSISSIPPI SUPREME COURT AND
THE MISSISSIPPI COURT OF APPEALS

Keep your office informed with a subscription to the *Recent Decisions of the Mississippi Supreme Court and Court of Appeals.* Briefs of the Mississippi Supreme Court and Mississippi Court of Appeals are written by Journal members and mailed by Tuesday of the week after the decisions are rendered, or e-mailed by Monday of the week after the decisions are rendered, several weeks before cases are printed in the regional reporter. You can receive this weekly publication and be up to date for $75 per year for hard copy; $65 per year for e-mail–an indispensable service! Subscribe now, or write for a free sample of the most current briefs.

Mississippi Law Journal
P.O. Box 849
University, Mississippi 38677-0849

# Robert C. Khayat Scholarship Endowment

The *Mississippi Law Journal* established the endowment in February of 1995 to honor the dedicated service of Robert C. Khayat, former Law Journal member, professor and current University Chancellor. The purpose of the endowment is to assist distinguished men and women of the *Journal* in the pursuit of their legal education at the University of Mississippi. As of July 1, 2005, the corpus of the endowment was $58,265.70. Each year deserving *Journal* members are awarded scholarships as selected by the Executive Board of the *Journal*. This year $1,000 was awarded to Journal members. Please help us increase the corpus of the endowment so that we can increase the number and size of these scholarships.

Checks should be made payable to and mailed to:

The University of Mississippi Foundation
Post Office Box 8288
University, MS 38677

Please note on your check that your gift is designated for the Robert C. Khayat Scholarship Endowment.

Contributions are tax deductible.

The *Mississippi Law Journal* is published four times during the school year, including a Special Edition published in the Fall. Editorial and business offices: Post Office Box 849, University, Mississippi 38677.

Current subscription: $35.00 per year. Single issue: $12.00. Subscriptions are renewed automatically upon expiration unless the subscriber sends a notice of termination.

Change of address: Send address changes directly to the *Mississippi Law Journal*. Include name, new address (including zip code) and old address. Please notify the *Journal* forty-five days in advance to ensure prompt delivery. Unless a claim is made for non-receipt of the *Journal* within six months after the mailing date, the *Mississippi Law Journal* cannot be held responsible for supplying those issues without charge. Third class postage paid at University, Mississippi 38677 and additional mailing offices.

Contributors are requested to submit manuscripts in 12-point font, double-spaced in hard copy form and on a 3.5" diskette in WordPerfect 8 or 10 or an easily convertible format. **Submissions may be sent electronically to: misslj@olemiss.edu. All mailed submissions should be addressed to:**

**Executive Articles Editor**
**Mississippi Law Journal**
**P.O. Box 849**
**University, MS 38677**

Citations should conform to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (18th ed. 2005).

The *Mississippi Law Journal* is a member of the National Conference of Law Reviews.

To offer its contributors complete freedom, the *Journal* assumes no responsibility for the views expressed herein.

Back issues of the *Mississippi Law Journal* may be ordered directly from William S. Hein & Co., Inc., 1285 Main Street, Buffalo, New York 14029-1987. Orders may also be placed by calling William S. Hein & Co., Inc. at (800) 828-7571, via fax at (716) 883-8100 or email to order@wshein.com. Back issues are also available in PDF format through HeinOnline.

# Administrative Officers of the University of Mississippi

| | |
|---|---|
| Robert C. Khayat | *Chancellor* |
| Carolyn Ellis Staton | *Provost and Vice Chancellor for Academic Affairs* |
| Gloria Kellum | *Vice Chancellor for University Affairs* |
| Alice Clark | *Vice Chancellor for Research and Sponsored Programs* |
| Johnny Williams | *Vice Chancellor for Administration and Finance* |
| Don Luis Frugé | *President/CEO, The University of Mississippi Foundation* |
| Timothy L. Hall | *Associate Provost* |
| Thomas Wallace | *Vice Chancellor for Student Life* |
| Andrew P. Mullins, Jr. | *Executive Assistant to the Chancellor* |
| Samuel M. Davis | *Dean of the School of Law, Director of Law Center, Jamie L. Whitten Chair of Law and Government and Professor of Law* |

## The Law School Faculty

Guthrie T. Abbott, *Professor Emeritus and Butler, Snow, O'Mara, Stevens and Cannada Lecturer in Law Emeritus*
Richard L. Barnes, *Professor of Law and Leonard B. Melvin, Jr. Distinguished Lecturer in Law*
Deborah H. Bell, *Professor of Law, Mississippi Defense Lawyers Association Distinguished Lecturer and Director of the Civil Legal Clinic*
John R. Bradley, *Professor of Law*
Phillip W. Broadhead, *Director, Clinical Appeals Program and Clinical Professor*
Charles Brower, II, *Croft Associate Professor of International Law and Jessie D. Puckett, Jr. Lecturer in Law*
Mercer E. Bullard, *Assistant Professor of Law*
Larry Bush, *Professor Emeritus of Law*
William M. Champion, *Professor Emeritus and Mississippi Defense Lawyers Association Distinguished Lecturer Emeritus*
Thomas K. Clancy, *Director of the National Center for Justice and the Rule of Law and Visiting Professor of Law*
George C. Cochran, *Professor of Law*
Aaron S. Condon, *Professor Emeritus of Law*
John M. Czarnetzky, *Associate Professor of Law and Mitchell, McNutt, and Sams Lecturer*
Donna Davis, *Associate Professor of Law*
Jason Derrick, *Acting Assistant Professor of Legal Writing*

KYLE DUNCAN, *Assistant Professor of Law*
THOMAS R. ETHRIDGE, *Professor Emeritus of Law*
D. MICHAEL FEATHERSTONE, *Professor Emeritus of Law*
MOLLY FERGUSSON, *Acting Assistant Professor of Legal Writing*
JOANNE I. GABRYNOWICZ, *Research Professor and Director of the National Remote Sensing and Space Law Center*
KRIS L. GILLILAND, *Director of Law Library and Assistant Professor of Law*
KAREN O. GREEN, *Professor of Law and Mississippi Defense Lawyers Association Distinguished Lecturer*
MATTHEW R. HALL, *Assistant Professor of Law*
TIMOTHY L. HALL, *Associate Provost and Professor of Law*
MARC HARROLD, *Counsel for National Programs and Visiting Professor of Law, National Center for Justice and the Rule of Law*
MICHAEL H. HOFFHEIMER, *Professor of Law and Mississippi Defense Lawyers Association Distinguished Lecturer*
ROBERT C. KHAYAT, *Chancellor and Professor of Law*
PATRICIA KRUEGER, *Acting Assistant Professor of Legal Writing and Director of Academic Excellence Program*
DON MASON, *Associate Director of the National Center for Justice and the Rule of Law and Lecturer*
KALI MURRAY, *Assistant Professor of Law*
GARY MYERS, *Professor of Law*
JACK W. NOWLIN, *Associate Professor of Law and Jessie D. Puckett, Jr., Lecturer*
E. FARISH PERCY, *Assistant Professor of Law*
LARRY J. PITTMAN, *Professor of Law and Jessie D. Puckett, Jr. Lecturer*
LISA S. ROY, *Assistant Professor of Law*
RONALD J. RYCHLAK, *Associate Dean for Academic Affairs, Professor of Law and Mississippi Defense Lawyers Association Lecturer*
PAUL M. SECUNDA, *Assistant Professor of Law*
JACQUELINE SERRAO, *Associate Director of the National Remote Sensing on Space Law Center*
HANS P. SINHA, *Director of Prosecutorial Externship Program and Clinical Professor*
CAROLYN ELLIS STATON, *Provost, Vice Chancellor for Academic Affairs and Professor of Law*
JULIE WATERSTONE, *Visiting Clinical Professor and Staff Attorney for the Civil Law Clinic*
MICHAEL WATERSTONE, *Assistant Professor of Law*
ROBERT A. WEEMS, *Professor of Law and Butler, Snow, O'Mara, Stevens and Cannada Lecturer in Law*
C. JACKSON WILLIAMS, *Director of Legal Writing Program and Acting Assistant Professor of Law*

Digitized by the Internet Archive
in 2012 with funding from
LYRASIS Members and Sloan Foundation

http://archive.org/details/mississippilawjo75susa

# MISSISSIPPI LAW JOURNAL

PUBLISHED BY STUDENTS AT THE
UNIVERSITY OF MISSISSIPPI
SCHOOL OF LAW

**VOLUME 75** **FALL 2005** **NUMBER 1**

COPYRIGHT © 2005 MISSISSIPPI LAW JOURNAL, INC.

*Editor-in-Chief*
GREGG MAYER

*Executive Editor*
PAUL M. ELLIS

*Articles Editors*
STEPHEN W. DUMMER
LANESHA L. SIMS
JAMES MATTHEW TYRONE

*Business Manager*
GINNY MASLIN

*Notes & Comments Editor*
HALLIE BOURLAND

*Mississippi Cases Editor*
A. MEAGHIN BURKE

*Symposium Editor*
ELIZABETH MILLS

*Membership Director*
KEISHUNNA L. RANDALL

ASSOCIATE EDITORS

*Articles Editors*
LEE WILL BERRY
MICHAEL BROUN
LAURA L. HILL
SHAWN MCCARVER
ALLISON MOODY
JESSE NELSON

*Mississippi Cases Editors*
MATTHEW PARKS
ELIZABETH PENN
PAUL B. WATKINS, JR.

*Notes & Comments Editors*
JASON BUSHBY
STEVEN KING

*Office Manager*
PATRICK H. STRONG

*Administrative Assistant*
PEGGY C. NAIL

*Faculty Advisors*
DEBORAH H. BELL
MATTHEW R. HALL
ROBERT A. WEEMS

## STAFF

Vicki Bobo
Casey Butts
Hyde Carby
Jake Dickerson
Jared Eastlack
Case Embry
Ed Everitt
Jonathan Festa
Joseph Gill
Michael Gorman
Loren Henagan
Katie Hill
Mary Clift Hitt
Nicholas Holtz
Alexandra Hutton
Joshua Kyle
Eleanor Laporte
Kara Lincoln
Vasilios Manthos
Kate Mauldin
Maggie Maynord
Ryan O'Beirne
David O'Neal
Eric Patterson
Ryan Pratt
Ronnie Wade Robertson
Nicole Seale
Jason Shields
Kathleen Shields
Ann Taylor
Slates Veazey
Kathryn E. Wetherbee
Nancy Williams

# National Center for Justice and the Rule of Law

*The University of Mississippi School of Law*

The National Center for Justice and the Rule of Law is a part of the University of Mississippi School of Law. The Center focuses on issues relating to the criminal justice system, with its purpose to promote the two concepts comprising the title of the Center. The concept of "justice" appeals to basic notions of equality, equity, and fairness, often with an emotive component. In contrast, the phrase "rule of law" refers to the requirement that certain procedures and principles must be followed in each case to reach a correct result. Neither concept is sufficient; rather, both must be utilized to ensure that the criminal justice system fulfills its function in society. The Center implements its mission through projects, conferences, educational programs, and publications that examine important criminal law and procedural issues.

Thomas K. Clancy
Director

The Center has five programs:

***National Programs Initiative***

Helps state governments investigate sophisticated criminal activity through training and model programs designed to attack computer-related crime.

***Fourth Amendment Initiative***

Promotes awareness of search and seizure principles through conferences, training, and support for selected publications.

***Prosecution Externship Program***

Provides specialized course-work and real-world training for law students in the duties and responsibilities of prosecutors.

***Criminal Appeals Clinic***

Provides law students with intensive training representing on appeal persons convicted of crimes.

***Special Projects***

Provides support for selected projects that promote the concepts of justice and the rule of law.

Visit the Center's website at www.NCJRL.org for additional information about these programs.

# Mississippi Law Journal

**Published by Students at the**
**University of Mississippi**
**School of Law**

---

**VOLUME 75** **FALL 2005** **NUMBER 1**

---

**Copyright © 2005 Mississippi Law Journal, Inc.**

## TABLE OF CONTENTS

### SYMPOSIUM

### THE SEARCH AND SEIZURE OF COMPUTERS AND ELECTRONIC EVIDENCE

FOREWORD . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . *Thomas K. Clancy* i

THE FOURTH AMENDMENT IN AN ERA OF UBIQUITOUS TECHNOLOGY
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . *Susan W. Brenner* 1

SEARCH WARRANTS IN AN ERA OF DIGITAL EVIDENCE
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . *Orin S. Kerr* 85

TRANSACTION SURVEILLANCE BY THE GOVERNMENT
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . *Christopher Slobogin* 139

THE FOURTH AMENDMENT ASPECTS OF COMPUTER SEARCHES AND SEIZURES: A PERSPECTIVE AND A PRIMER
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . *Thomas K. Clancy* 193

COMPUTER SEARCHES OF PROBATIONERS—DIMINISHED PRIVACIES, "SPECIAL NEEDS" & "'*WHILST' QUIET* PEDOPHILES"—PLUGGING THE FOURTH AMENDMENT INTO THE "VIRTUAL HOME VISIT"
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . *Marc M. Harrold* 273

# FOREWORD

# THE SEARCH AND SEIZURE OF COMPUTERS AND ELECTRONIC EVIDENCE

*Thomas K. Clancy*[*]

The National Center for Justice and the Rule of Law,[1] a program of the University of Mississippi School of Law, focuses on issues relating to the criminal justice system, with its purpose to promote the two concepts comprising the title of the Center. In furtherance of its mission, the Center has established the *Fourth Amendment Initiative*. Perhaps no other Amendment has such broad applicability to everyday life as does the Fourth Amendment. The Fourth Amendment is also a very complicated area of jurisprudence and the legal landscape is constantly changing as a result of new technology and court decisions. The purpose of the Center's initiative is to promote awareness of Fourth Amendment principles through conferences, publications, and training of professionals in the criminal justice system. The Center takes no point of view as to the direction that Fourth Amendment analysis should take but seeks to facilitate awareness of the issues and encourage discussion of search and seizure principles.

---

[*] Director, National Center for Justice and the Rule of Law, and Visiting Professor, University of Mississippi School of Law.

[1] The National Center for Justice and the Rule of Law is supported by a grant from the Bureau of Justice Assistance, Office of Justice Programs, of the U.S. Department of Justice, grant No. 2000-DD-VX-0032. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in the articles stemming from this symposium are those of the author and do not represent the official position of the United States Department of Justice. For more information about the Center, please visit www.ncjrl.org.

A central pillar of the Fourth Amendment Initiative is annual symposiums on important search and seizure topics. On February 17, 2005, the Center held its fourth annual symposium, *The Search and Seizure of Computers and Electronic Evidence*. The symposium coincided with the third day of a conference entitled *Advanced Training on Search and Seizure of Computers and Obtaining Electronic Evidence*, sponsored by the Center in cooperation with the National Association of Attorneys General, which was attended by approximately 64 prosecutors and others, from Attorneys General offices from 34 states, American commonwealths, and territories; for the symposium, they were joined by 55 lawyers, law students, and law professors, while another 219 persons observed the symposium via the Internet.

The Center believes that the conference and symposium–and the insightful articles published in this special edition of the *Mississippi Law Journal* that stemmed from the presentations at those events–significantly further the Center's mission and, more importantly, make significant contributions to the understanding of Fourth Amendment principles. The Center, and I personally, wish to thank the leading legal scholars who participated.

Susan Brenner, Professor at the University of Dayton School of Law, in her article, *The Fourth Amendment in an Era of Ubiquitous Technology*, poses the question whether the guarantee of privacy contained in the Fourth Amendment is adaptable to a world where technology is "increasingly pervasive–a world of ubiquitous technology." In answering the question, Brenner examines how the approach to privacy, which began as a "bricks and mortar" concept, evolved in the 20th Century to accommodate technological change. Brenner observes that the physical and informational barriers that once served to differentiate our public and private lives are rapidly being eroded by technology. Thus, Brenner maintains, a spatial conception of the guarantee offered by privacy is no longer effective. Brenner offers insights on how to adapt the concept of privacy to accommodate the challenges of the 21st Century, that is, to a society where physical barriers have little, if any, meaning. An essential feature of information technology is the ability of others to "harvest" that information and Brenner discusses impediments to protecting such information, including the concepts of voluntary exposure and assumption of risk; she argues that the assumption of risk "calculus is an unreasonable methodology for a non-spatial world." Brenner, after observing that society acknowledges privacy protections for certain types of shared privacy, proposes expanding that concept to include information conveyed to "servant" entities who provide us with various types of support.

Orin Kerr, an Associate Professor at The George Washington School of Law, in his article *Search Warrants in an Era of Digital Evidence*, contends that the legal rules regulating the search warrant process must be revised in light of the demands of digital evidence collection. He asserts that existing rules are premised on the police obtaining a warrant to enter the place to be searched and then retrieving the property named in the warrant. Computer technologies, Kerr believes, tend to bifurcate the process into two steps: the police must first execute a physical search to seize the computer hardware and then later execute a second electronic warrant to obtain the data from the seized computer storage device. He asserts that the law has failed to account for that two-stage process and, hence, regulate the warrant process effectively. Kerr offers a series of proposed amendments to Rule 41 of the Federal Rules of Criminal Procedure to update the warrant process for the era of digital evidence.

Christopher Slobogin, a Professor at the University of Florida Fredric G. Levin College of Law, in *Transaction Surveillance by the Government*, observes that many important aspects of our lives are inscribed in written and digitized records, housed in private businesses, government agencies, and other institutions. The records include all sorts of information about us: reports on our medical status and financial condition; data about our purchases, rentals, real estate holdings, licenses, and memberships; logs listing the destination of our emails and our Internet wanderings; and countless other bits of individual descriptors, ranging from salary levels to college grades to driver's license numbers. Slobogin notes that there is often an understanding that the information will be used or viewed by a limited number of people for circumscribed purposes, that is, we consider the contents of many of the records private. His article explores what he calls "transaction surveillance" by the government, which involves accessing already-existing records, either physically or through computer databanks, and accessing the identifying signals of a transaction (such as the address of an email recipient). Slobogin observes that transaction surveillance is subject to far less regulation than either physical surveillance of activities inside the home or communications surveillance. He argues that transaction surveillance should be subject to much more legal monitoring than it is. He proposes recognizing that different sorts of records merit different levels of protection, significantly increasing the degree of protection to the probable cause level for personal records held by private and public entities and to the reasonable suspicion level for records readily available to the public. Although Slobogin examines several alternative approaches to affording protections to records, including legislative action, he concludes that only the Fourth Amendment, properly construed, has the ability to provide adequate protection.

In *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, I offer a "primer" that outlines the application of Fourth Amendment principles to the search and seizure of computers and the digital information that is stored in them. The article, however, departs from the role of a primer in two important respects. First, in discussing the nature of computer and digital evidence searches and seizures, it rejects the view that unique Fourth Amendment rules are needed to regulate them; instead, I believe that computers are containers and the data they contain are mere forms of documents. This is to say that the principles applicable to document searches have equal application to electronic data searches. Second, the article rejects expansion of the private search doctrine, used by some courts to permit government agents to open data files that had not been opened during a preceding private party search and still not be a search within the meaning of the Fourth Amendment. Underlying both of these points of view is the perspective that a computer is a container of containers of documents, that is, each individual file is a separate container–just like each manila file in a filing cabinet is a container–that requires a separate opening to determine what is inside. This is to say that the mere fact that an item to be searched or seized is electronic evidence does not fundamentally change the Fourth Amendment analytical structure that governs.

Marc Harrold, who is Counsel for National Programs at the Center and a Visiting Professor at the University of Mississippi School of Law, writes *Computer Searches of Probationers—Diminished Privacies, "Special Needs"* & "'Whilst' Quiet *Pedophiles"—Plugging the Fourth Amendment into the "Virtual Home Visit."* This is an important topic, given the large number of child sex offenders and child pornographers who use the Internet to facilitate their crimes. Harrold discusses the Fourth Amendment framework that regulates governmental programs that monitor the computer and Internet use of persons on probation. He surveys the various technological and other tools that are available to facilitate that monitoring. Harrold examines the Supreme Court and lower court decisions in the area and concludes that the "special needs" doctrine, developed by the Supreme Court to assess the reasonableness of regulatory and other searches, will most likely serve as the basis of assessing the reasonableness of the searches of probationers' computers.

# THE FOURTH AMENDMENT IN AN ERA OF UBIQUITOUS TECHNOLOGY

*Susan W. Brenner*[*]

## I. Privacy

> *We must think through the way technology changes what is private, and develop new concepts of reasonable privacy that preserve liberty and are workable in a networked world.*[1]

The pre-eminent guarantee of personal privacy for those of us in the United States is the Fourth Amendment to the United States Constitution. As most everyone knows, the Fourth Amendment protects us from "unreasonable" searches and seizures. Searches infringe upon privacy; seizures impact on other interests, notably the interest in the possession and use of property.[2]

Privacy evolved as a "bricks and mortar" concept.[3] When the Fourth Amendment was added to the Constitution, the real-world was the only world; technology had not yet given us the ability to transcend the strictures of the real-world in various ways.[4] We now have that ability: We can substitute the virtual realities provided by computer technology for the physical world; we can communicate with almost anyone from almost anywhere; and we use technologies to make our lives easier, to earn our living and to amuse us.

---

[*] NCR Distinguished Professor of Law and Technology, University of Dayton School of Law.

[1] *Elon University/Pew Internet & American Life Project, Imagining the Internet: Predictions Database*, Fall 2004 at http://www.elon.edu/predictions/q12.aspx (last visited Aug. 2005). In 2004, the Pew Internet & American Life Project surveyed "1,286 network-technology stakeholders" to elicit their views as to how the Internet "will change our lives between 2004 and 2014." *Id.* The comment quoted in the text above was one respondent's reaction to this question:

> As computing devices become embedded in everything from clothes to appliances to cars to phones, these networked devices will allow greater surveillance by governments and businesses. By 2014, there will be increasing numbers of arrests based on this kind of surveillance by democratic governments as well as by authoritarian regimes.

*Id.*

[2] *See, e.g.*, United States v. Karo, 468 U.S. 705, 728 (1984) (Stevens, J., concurring in part and dissenting in part).

[3] The phrase "bricks-and-mortar" "[d]escribes a site that has a physical pres-

Technology is not a new phenomenon; ancient inventors produced complex mechanisms and understood a great deal about the physical forces underlying modern technology.[5] What is new is the way we approach technology: Ancient inventions were regarded as curiosities and often remained little more than toys;[6] this tendency to ignore or resist new technologies, which was the product of various social and cultural forces, persisted for centuries.[7] The resistance began to decline in the nineteenth century because of the implementation of technologies—including the telegraph, electricity, the telephone, and the automobile—that would proliferate and permeate the fabric of society.[8] The success of these and subsequent

---

ence in the real world (as opposed to a virtual presence in the online world)". WordSpy, Definition of bricks-and-mortar, at http://www.wordspy.com/words/bricks-and-mortar.asp (last visited Aug. 2005).

[4] NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 79-105 (1937).

[5] *See, e.g., The Antikythera Mechanism: The Clockwork Computer*, THE ECONOMIST (Sept. 19, 2002), at http://www.economist.com/displaystory.cfm?story_id=1337165 (last visited Aug. 2005); Ancient Greek Scientists: Hero of Alexandria, Technology Museum of Thessaloniki, at http://www.tmth.edu.gr/en/aet/5/55.html (last visited Aug. 2005) (hero invented the steam engine, among other things, in the first century B.C.); *see also* RUDI VOLTI, SOCIETY AND TECHNOLOGICAL CHANGE 35-44, 54-56 (4th ed. 2001).

[6] *See, e.g.,* A. WOLF, A HISTORY OF SCIENCE, TECHNOLOGY AND PHILOSOPHY IN THE 16TH AND 17TH CENTURIES 543 (1935); *see also* WILLIAM FIELDING OGBURN, TECHNOLIGICAL TRENDS AND NATIONAL POLICY, INCLUDING THE SOCIAL IMPLICATIONS OF NEW INVENTIONS 51 (1937).

[7] *See, e.g.,* OGBURN, *supra* note 6, at 66 ("resistance to technological change has been so much a part of the texture of the historical process, that it cannot be ignored when the future of technology is charted"). *See id.* at 39-66 (describing historical resistance to different technologies).

[8] *But see id.* at 43-45, 49-51 and 53 (early resistance to these technologies).

technologies produced a cultural climate which embraced new technology.[9] Our receptivity to technology accelerates the processes of invention and implementation which, in turn, influence how we live; we move further and further away from the "bricks and mortar" reality that produced the Fourth Amendment.[10]

And that brings us to the question at hand: Can the Fourth Amendment's privacy guarantees be adapted to deal with a world in which technology is increasingly pervasive—a world of ubiquitous technology?[11]

To answer that question, we must do several things: The first is to identify the basic conceptions of privacy which existed in Twentieth Century American law: the Fourth Amendment standard and a tort standard derived from the work of Louis Brandeis and Charles Warren. The two sections immediately below undertake this analysis,[12] the purpose of which is to provide a benchmark—to let us understand how our approach to privacy evolved to accommodate technologies. The next step is to adapt that approach to accommodate Twenty-first century technologies. Section II of the article reviews existing and projected technologies and explains why the approach which evolved is inadequate. Section III considers how we can adapt our approach to deal with the era of ubiquitous technology. Finally, Section IV offers a brief conclusion.

---

[9] *See, e.g.*, STEVEN JOHNSON, INTERFACE CULTURE: HOW NEW TECHNOLOGY TRANSFORMS THE WAY WE CREATE AND COMMUNICATE 1-10 (1st ed. 1997); *see also* VOLTI, *supra* note 5, at 35-53, 266-68.

[10] *See* Section I.A., *infra.*

[11] The phrases "ubiquitous technology" and "ubiquitous computing" are used interchangeably to refer to technologies that are woven into the fabric of everyday life. *See, e.g.*, Niall Winters, *Personal Privacy and Popular Ubiquitous Technology*, UbiConf 2004, at http://www.uclic.ucl.ac.uk/projects/ubiconf/materials/Papers/Niall%20Winters.pdf. (last visited Aug. 2005). John Blau notes:

> Ubiquitous computing involves having computing devices essentially everywhere in the home, office or public area, as well as easy, natural ways for people to interact with them. Wireless technologies, sensors, radio frequency identification (RFID) tags and machine-to-machine communications will play a big role in this new area of computing.

John Blau, *German Group Studies Ubiquitous Computing, Data Privacy*, Network World, Dec. 22, 2004, at http://www.nwfusion.com/news/2004/1222germagroup.html (last visited Aug. 2005). This article focuses on "communicative" technologies instead of, say, industrial or agricultural technologies. Its concern is with technologies that can be used to generate information, collect information and/or share information. *See* Section II., *infra.* The Fourth Amendment is, of course, concerned with channeling how law enforcement finds, through searches, and obtains, through seizures, varieties of information. *See* Section I.A., *infra.*

[12] *See infra* §§ I(A) and I(B),

### A. *Fourth Amendment*

> *The . . . constitutional prohibition against unreasonable searches and seizures, has its source in that principle of the common law which finds expression in the maxim that 'every man's house is his castle.' English history discloses [that the] . . . constitutional provisions . . . had their origin 'in the . . . unwarrantable intrusion of executive agents into the houses . . . of individuals . . . .'"*[13]

The Fourth Amendment is predicated on a spatial conception of privacy.[14] It is intended to protect the sanctity of private property from intrusions by public officials[15] which derives from English common law.

Early common law punished "those who invaded a neighbor's premises."[16] In fact, by the Twelfth-century, housebreaking had become one of the "more serious crimes in medieval England" and by the Sixteenth-century English law had developed specific prohibitions against housebreaking, burglary and trespass.[17] These laws were only concerned with trespasses by private persons because official searches were almost unheard of until the Fifteenth century.[18] In the latter half of the Fifteenth century, however, the King and Parliament began authorizing trade guilds to "enter and search the workmanship of all manner of persons" to enforce guild regulations.[19] Roughly a century later, the Court of the Star Chamber, charged with licensing books and regulating printing "decreed that the wardens of the Stationers' Company . . . should have authority to open all packs and trunks of papers and books brought into the country, to search in any warehouse, shop, or any other place where they suspected a violation of the laws of printing to be taking place [and] to seize the books printed contrary to law".[20] Other courts followed suit, issuing edicts authorizing similar searches directed at those suspected of libel, heresy and political dissent.[21] This led to the evolution of the general warrant, which was issued with no proof of individualized suspicion and in which no "names are specified . . . and . . . a discretionary power given to messengers to search wherever their suspicions may chance to fall."[22] As arbitrary searches became more common, "Englishmen began to insist that their houses were castles for the paradoxical reason that the castle-like security that those houses had afforded from intrusion was vanishing."[23]

---

[13] United States v. Three Tons of Coal, 28 F. Cas. 149, 151 (E.D. Wis. 1875). English law, of course, was not alone in providing special protection for the home. *See* LASSON, *supra* note 4, at 13-20.

[14] *See* Olmstead v. United States, 277 U.S. 438, 463 (1928) ("The well-known historical purpose of the Fourth Amendment . . . was to prevent the use of governmental force to search a man's house, his person, his papers, and his effects.").

[15] *See* Boyd v. United States, 116 U.S. 616, 627 (1886).

[16] *See* William J. Cuddihy, *The Fourth Amendment: Origins and Original Meaning* 32 (1990) (unpublished Ph.D. dissertation, Claremont Graduate School) (on file with author).

[17] *Id.* at 31-35.

---

[18] *Id.* at 36, 75. A law enacted in 1335 required innkeepers near ports to search guests for counterfeit money; the innkeepers kept a portion of whatever they found and turned the rest over to "official searchers" who took the rest and monitored the innkeepers' discharge of this obligation. *See* LASSON, *supra* note 4, at 23.

[19] *See* LASSON, *supra* note 4, at 24.

[20] *Id.* at 25. The Stationers' Company was a guild of printers charged with enforcing the Star Chamber's restrictions on printing. *See, e.g.,* TELFORD TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION 25 (1969).

[21] *See* LASSON, *supra* note 4, at 25-27.

> No limitations seem to have been observed in giving messengers powers of search and arrest in ferreting out offenders and evidence. Persons and places were not necessarily specified, seizure of papers and effects was indiscriminate, everything was left to the discretion of the bearer of the warrant.

*Id.* at 26; *see also* Cuddihy, *supra* note 16, at 100-19.

[22] LASSON, *supra* note 4, at 45 (quoting Wilkes v. Wood, 98 Eng. Rep. 489 (C.D. 1763)).

In several decisions issued in the mid-eighteenth century, English courts held that homes were protected from arbitrary action by government officials.[24] Most of these decisions grew out of an investigation into seditious libel: Ordered to find the author of a recently-published letter, officers acting under the authority of a general warrant searched five houses and made a number of arrests.[25] Those persons whose homes were searched sued the officers who conducted the searches for trespass, and the government "undertook the responsibility of defending all actions arising from the warrant and the payment of all judgments."[26] To the delight of the British public, the plaintiffs won, and their verdicts were upheld on appeal.[27] Encouraged by their success, John Entick, the victim of a similar search, sued the officers who searched his home for trespass and won a verdict of £300.[28] The Court of Common Pleas upheld his verdict:

> [O]ur law holds the property of every man so sacred that no man can set his foot upon his neighbour's close without his leave. [If] he does, he is a trespasser. . . . The defendants have

---

[23] Cuddihy, *supra* note 16, at 128; *see also* LASSON, *supra* note 4, at 30-45.

[24] *See* Money v. Leach, 97 Eng. Rep. 1050 (K.B. 1765); Entick v. Carrington, 95 Eng. Rep. 807 (K.B. 1765); *Wilkes*, 98 Eng. Rep. at 489; Huckle v. Money, 95 Eng. Rep. 768 (K.B. 1763).

[25] *See* Cuddihy, *supra* note 16, at 886-94; *see also* LASSON, *supra* note 4, at 43-45.

[26] LASSON, *supra* note 4, at 45.

[27] *Id.* at 44-46.

[28] *Id.* at 47; *see also Entick*, 95 Eng. Rep. at 808:

> The plaintiff . . . declare[d] that the defendants [Nathan Carrington and three others, messengers in ordinary to the King] with force and arms broke and entered his dwelling-house . . . , continued there four hours without his consent and against his will, all that time disturbed him in the peaceable possession thereof, broke open the doors to the rooms, and the locks, . . . broke open the boxes, chests, drawers, etc., of the plaintiff in his house, . . . searched and examined all the rooms . . . in his dwelling . . . and all the boxes . . .; read over, pried into, and examined all the private papers . . . of the plaintiff there found, whereby the secret affairs, etc., of the plaintiff became wrongfully discovered and made public. . . to the damage of the plaintiff, 2,000 pounds.

*Id.*

> no right to avail themselves of the usage of these warrants. . . . [W]e can safely say there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society.[29]

The effect of these decisions was to apply the same standard to public and private actors: In either instance, a trespasser could be held civilly liable for entering another's property "without lawful authority".[30] The primary difference was that a public actor could rely upon a warrant, as well as upon a property owner's consent, as authorization for an entry.[31]

During this era, American colonists were waging their own war against writs of assistance, a variant of the general warrant.[32] Although their legal challenge to the writs failed,[33] the resentment generated was a driving factor for the Revolution and, later, in the adoption of the Bill of Rights.[34] The Fourth Amendment was therefore a product of the same concerns that resulted in the law of trespass' being applied to public actors: "to guard individuals against improper intrusion into their buildings where they had the exclusive right of possession".[35] It was intended to secure spatial privacy—to restrict law enforcement's ability to break down doors and rummage through rooms, boxes, chests, drawers, etc.[36] Like its English analogue, the Fourth Amendment was intended to preserve privacy by discouraging law enforcement trespasses,[37] and that conception of privacy prevailed unchallenged until the second decade of the Twentieth century when the Supreme Court heard its first wiretap case.

---

[29] *Entick*, 95 Eng. Rep. at 818.

[30] WILLIAM BLACKSTONE, III, COMMENTARIES ON THE LAWS OF ENGLAND 209 (1870).

[31] As one scholar noted, a warrant "would act as a sort of declaratory judgment . . . . A lawful warrant . . . would compel a . . . directed verdict for the defendant government official in any subsequent lawsuit for damages." Akhil Reed Amar, *The Bill of Rights As A Constitution*, 100 YALE L.J. 1131, 1178-79 (1991); *see also* Patcher v. Sprague, 1807 WL 931 (N.Y. 1807) (valid warrant is a defense to an action for trespass).

[32] *See* LASSON, *supra* note 4, at 53 (with a writ of assistance one could "search any house, shop, warehouse, etc.; break open doors, chests, packages . . . and remove any prohibited or uncustomed goods or merchandise").

[33] *Id.* at 51-61.

[34] *Id.* at 79-82; *see also* Marshall v. Barlow's, Inc., 436 U.S. 307, 311 (1978).

[35] Jones v. Gibson, 1818 WL 488 *5 (N.H. 1818).

[36] *See supra* note 28.

There were only a few Fourth Amendment cases in the Nineteenth century and perhaps the best known is *Boyd v. United States*. *Boyd* involved the "compulsory production of a man's private papers," which the Court found to be the "equivalent" of a search and seizure.[38] The Court struck down the practice in an opinion which cited *Entick* and seemed to fuse the Fifth Amendment's privilege against self-incrimination with the Fourth Amendment's prohibition against "unreasonable searches and seizures."[39] The opinion quotes *Entick* extensively for the proposition that an unauthorized violation one's "papers" is a trespass.[40] The focus was on spatial privacy—on the government's "*going*" or "*seeing*" something it should not—even though the "intrusion" was accomplished indirectly.[41]

---

[37] *See, e.g.,* Humes v. Taber, 1850 WL 1823 *6 (R.I. 1850) (warrant no defense to an action in trespass against a sheriff who searched the wrong house); *Jones*, 1818 WL at *5 (action in trespass against an "inspector of revenue" for seizing goods without a warrant); Patcher v. Sprague, 1807 WL 931 (N.Y. 1807) (valid warrant is a defense to an action for trespass).

[38] *Boyd*, 116 U.S. at 622. A court order was used to require "the claimants" in the case to surrender an invoice concerning the purchase of 29 cases of plate glass. *Id.* at 617-18. Order issued as part of an investigation into whether "the claimants" had unlawfully avoided paying duties on the glass. *Id.*

[39] *Id.* at 632-35.

[40] *Id.* at 626-30.

[41] *See supra* note 38. The Supreme Court cited *Boyd*'s Fourth Amendment-Fifth Amendment fusion analysis in several cases, none of which involved the traditional Fourth Amendment scenario in which the government searches for and seizes evidence. *See* Bram v. United States, 168 U.S. 532, 544 (1897) (coerced confession case); Stone v. United States, 167 U.S. 178, 188 (1897) (action to recover damages for trees unlawfully cut on federally-owned land); Brown v. Walker, 161 U.S. 591, 635-36 (1896) (grand jury witness' appeal of contempt citation for refusing to answer questions put to him); Counselman v. Hitchcock, 142 U.S. 547, 580-81 (1892) (grand jury witness' appeal of contempt citation for refusing to answer questions put to him), *overruled in part by* Kastigar v. United States, 406 U.S. 441 (1972). *See generally* United States v. Zucker, 161 U.S. 475, 478 (1896). Many of these cases, along with some lower federal court decisions from this era, involved compelling testimony from witnesses. *See, e.g., In re* Jefferson, 96 F. 826, 828 (D. Wash. 1899) (compelling witness to testify against her husband would

### 1. Letters

The most relevant Nineteenth-century Supreme Court decision is *Ex parte Jackson*,[42] which was an appeal from a conviction for sending "a circular concerning a lottery" through the U.S. Mail.[43] In *Jackson*, the Court held that Congress had the power to prohibit mail from being used to deliver certain types of material as long as the restrictions were enforced in accordance with rights of:

> far greater importance than the transportation of the mail. . . . [A] distinction is to be made between different kinds of mail matter,—between what is intended to be kept free from inspection, such as letters, and sealed packages subject to letter postage; and what is open to inspection, such as newspapers, magazines, . . . and other printed matter, purposely left in a condition to be examined. Letters and sealed packages . . . are as fully guarded from examination and inspection, except as to their outward form and weight, *as if they were retained by the parties forwarding them in their own domiciles*. The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures *extends to their papers, thus closed against inspection, wherever they may be*. Whilst in the mail, they can only be opened and examined under like warrant, issued upon . . . oath or affirmation, particularly describing the thing to be seized, *as is required when papers are subject-*

---

violate Fourth Amendment). David Steinburg writes:

> Federalism may in part explain the lack of early decisions interpreting the Fourth Amendment. In the eighteenth century and the nineteenth century, the Bill of Rights-including the Fourth Amendment-only applied to the federal government. During this same time period, most criminal laws were enacted by the states, not the federal government. Criminal prosecutions almost always took place in the state courts, where the Fourth Amendment did not apply.

David E. Steinberg, *The Original Understanding of Unreasonable Searches and Seizures*, 56 FLA. L. REV. 1051, 1072-73 (2004) (footnotes omitted); *see, e.g.*, Miller v. Texas, 153 U.S. 535, 538 (1894).

[42] 96 U.S. 727 (1877).

[43] *Id.*

> *ed to search in one's own household*. . . . [A]ll regulations adopted as to mail matter . . . must be in subordination to the great principle embodied in the fourth amendment of the Constitution.[44]

To the modern eye, *Jackson* seems to extract a concept of "portable privacy" from the notion of spatial privacy upon which the Fourth Amendment was predicated. Sealed letters and packages carry with them the privacy accorded the premises from which they originated; violating that privacy is a trespass which must be authorized by a warrant.[45] This appears to extend the original Fourth Amendment understanding of privacy as "privacy of place," to transcend the bricks-and-mortar approach meant to limit law enforcement intrusions into "private" physical spaces. To us, *Jackson* seems to anticipate *Katz*,[46] the Twentieth-century decision in which the Court expanded the Fourth Amendment to privacy beyond "space."[47]

It is doubtful that the *Jackson* Court viewed its holding in that light. It is more probable that the Court simply believed it was extending spatial privacy to "papers" which were in transit from one person to another—that were moving from one "private" space to another. Viewed in this light, the decision is but an application of the concern with spatial privacy and with the confidentiality of private "papers" that appears in *Entick* and the other English trespass decisions.[48] This interpretation is also supported by *Boyd*'s concern with non-traditional trespass into the privacy of one's "papers."[49]

But certain aspects of *Jackson* are still relevant to this discussion. For one thing, while *Jackson* did not specifically involve technology, it did provide the factual predicate for the holding. The colonial era postal service was ad hoc, notoriously unreliable and offered no guarantees that what was sent would not be read by government authorities, postal employees or anyone who happened to have access.[50] The situation did not seem to improve much after the Revolution, with the establishment of a formal postal service.[51] In a letter to the Marquis de Lafayette, soon-to-be President George Washington observed that sending a letter through the post office meant that his words "should become known to all the world."[52] By the nineteenth century, postal employees were at least trying to maintain the "secrecy" of communications sent through the mail.[53] Interestingly, as Smith notes:

---

[44] *Id.* at 728 (emphasis added).

[45] *See supra* notes 37, 44 and accompanying text.

[46] 389 U.S. 347 (1967).

[47] *Katz* is discussed *infra*. *See infra* notes 117-127 and accompanying text.

[48] *See supra* note 28.

[49] *See supra* notes 40-41 and accompanying text.

> [the] greatest protection for postal secrecy came not from a law or regulation, but from a physical innovation. In the mid-1800s adhesive envelopes were introduced, providing for the first time an easy means for sealing one's personal writings before entrusting them to the postal service.[54]

The self-sealing adhesive envelope was much more effective than its precursor, the wax-sealed envelope.[55] Thus, the *Jackson* Court's distinction between sealed mail and other material was made possible by an innovation in communications technology.

---

[50] *See* ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 23-26, 49-52 (2000). Colonists who were concerned about prying by Crown authorities developed codes to encrypt their letters. *Id.* at 24-26.

[51] *Id.* at 49-50.

[52] *Id.* at 50.

[53] *Id.* at 51-52.

> During the Nineteenth Century, it was the task of the Post Office to wipe out a tradition dating back to pre-Revolutionary times that intercepting mail and reading it was not especially uncommon—and to replace it with a new respect for confidential treatment of letters in transit. At mid-century, the task was not yet complete.

*Id.* at 54-55.

[54] *Id.* at 56.

[55] An 1873 New York Times editorial noted that a letter "'sealed with its red wafer, and into which the prying eyes of the village postmistress so often peeped, was soon superseded by the envelope, which secured the inviolability of the contents from all eyes but those for which they were intended." *Id.* at 56.

Another pertinent aspect of *Jackson* was its focus on the privacy of communications. The mode of communication at issue in *Jackson* was not new but an innovation made it reasonable, for the first time, to expect that the contents of letters and parcels could be protected from "snoops and other members of the public."[56] Whatever its import for Fourth Amendment jurisprudence, this development is significant because it parallels issues which were arising regarding contemporaneous technology, and anticipating issues which would develop regarding evolving technology.

### 2. Telegraphy

In 1844, Samuel Morse sent the first public telegram using technology he developed in 1836.[57] After Morse formed his telegraph company, Western Union, in 1845, the growth of "the telegraph network was . . . explosive."[58] As lines were strung around the world, telegraphy "revolutionized business practice, gave rise to new forms of crime, and inundated its users with information."[59] For practical reasons, telegraphy did not give rise to the privacy issues that had arisen with regard to materials sent through the mail. Unlike the postal system, telegraphy was a proprietary communication system where the contents of communications were revealed to agents of the telegraph company, who translated the messages into Morse Code and transmitted them to another agent, who translated them back from Morse Code and then delivered them to the recipient.[60] The lack of an analogue to the sealed envelope meant it

---

[56] California v. Greenwood, 486 U.S. 35, 40 (1988).

[57] SMITH, *supra* note 50, at 66; *see also* TOM STANDAGE, THE VICTORIAN INTERNET: THE REMARKABLE STORY OF THE TELEGRAPH AND THE NINETEENTH CENTURY'S ON-LINE PIONEERS vii (1998).

[58] *Id.* at 56-91.

[59] *Id.* at vii.

[60] *Id.* at 63-65.

> Whatever personal information or sentiments were included in the message truly left the control of the originator. Further, unlike the situation with the U.S. Mail, an employee handling telegraph traffic could easily

was not reasonable for those who employed telegraphy to claim that the privacy of their communications had been compromised by "insiders"—Western Union employees.[61]

There were, however, efforts to prevent the disclosure of telegram contents to "outsiders." Some states made it a crime for a telegraph company or its employees to disclose the contents to anyone but the authorized recipient.[62] Some also

---

> read messages without risking leaving the traces of an unopened envelope. There was no physical evidence of an interception. And, unlike the postal service, the telegraph system permitted the retention of every message.

SMITH, *supra* note 50, at 66; *see also* Arthur W. Grumbine, *The Era of Morse Telegraphy: Part 1*, at http://www.faradic.net/~gsraven/telegraph_tales/grumbine/grumbine_1.html (last visited Aug. 2005) ("[Telegraphy] was no different from opening everybody's mail and reading every word of it; then sending the contents across country by a peculiar code system invented by Samuel F. B. Morse").

[61] It would seem, of course, that messages could be encrypted to preserve the privacy of their contents, but this did not become a common practice:

> When it was first introduced, many people anticipated that telegraphic transmission would be far more secure than the Postal Office had been and that it would provide "impenetrable secrecy," because the messages were coded, or could be coded. But coding was not used for most business and personal correspondence. (The main reason was that a sender could recover damages caused by errors in transmission by the telegraph company but when it transmitted encoded messages its liability was significantly lower).

SMITH, *supra* note 50, at 67. *See, e.g.,* Primrose v. W. Union Tel. Co., 154 U.S. 1, 4-5 (1894) (suit seeking damages for mistake made in transmitting coded telegraphic message); Postal Tel.-Cable Co. v. Louisville Cotton Oil Co., 122 S.W. 852, 852-53 (Ky. Ct. App. 1909) (suit for damages resulting from failure to deliver coded telegraphic message). Criminals sometimes encrypted messages used to facilitate criminal activity. *See, e.g.,* State v. Chapman, 1871 WL 3337, at *5 (Nev. 1871) (accomplice sent a "cipher telegram" advising robbers when a large shipment of coins would be arriving).

[62] *See* MINN. GEN. STAT. § 6782 (1894) (cited in Peterson v. W. Union Telegraph Co., 77 N.W. 985, 987 (Minn. 1899); 13 WAGNER'S STATUTES § 51 (cited in *Ex parte* Brown, 1880 WL 423, at *4 (Mo. 1880)); *see also* Little Rock & Fort Smith Tel. Co. v. Davis, 1883 WL 1201, at * 3 (Ark. 1883) (noting state statutes imposing civil liability and criminal penalties) (citing SCOTT & JARNAGAN, LAW OF TELEGRAPHS §§ 419-46). The efficacy of these laws, which were enacted in "a bare majority" of states," is uncertain. *See, e.g.,* SMITH, *supra* note 50, at 68. A *New York Times* editorial from 1866 claimed that violations of these laws were hard to detect and that Western Union employees were subject to "'strong temptations'" to ignore them. *Id.* (quoting *The New York Times,* December 31, 1866, at 4).

adopted statutes creating a cause of action for those whose messages went awry or were otherwise made public.[63] Some observers were concerned about the possibility that Western Union would disclose the contents of messages to authorities. This became a reality in 1877, when a Congressional committee, investigating the validity of votes cast in certain states, sought access to telegrams as evidence.[64]

> Western Union President William Orton ordered [his employees] not to respond. He accused Congress of requiring his employees 'to become spies and . . . informers against the customers who have reposed in us the gravest confidence concerning both their official and their private affairs.' . . . With Democrats supporting disclosure and Republicans supporting confidentiality, the Western Union manager was found in contempt of Congress . . . arrested by a deputy sergeant of arms on Capitol Hill and detained.[65]

Orton eventually gave in; Western Union delivered "30,000 political telegrams . . . to the House Committee on Privileges and Elections in the winter of 1877."[66]

The messages, however, were never used in the investigation,[67] but the episode sparked a debate about the confidentiality of telegrams. Congressman James Garfield argued for legislation guaranteeing confidentiality, but other members of Congress believed that the "'security of society'" was more important than confidentiality.[68] Over the next few years, Congress debated whether telegrams "should be compared to Post Office material and therefore kept confidential" or "should be available by subpoena."[69] For the public, confidentiality "was a double-edged sword: a requirement of non-disclosure or of instant destruction of messages would protect privacy but also allow the company to escape liability for errors", since the evidence would have been destroyed.[70] Western Union responded by reducing the retention time for copies of messages, and in 1880 a House Committee "reported out favorably a bill . . . to protect telegrams to the very same extent as sealed letters in the Post Office."[71] The House did not act on the bill and the proposal died, in part because of events occurring elsewhere.[72] In 1880, Jay Gould, "perhaps the most hated capitalist of America's Gilded Age," acquired Western Union.[73] The public's distrust of Gould led to demands that the government take over Western Union, both to prevent price gouging and to protect the privacy of telegraphic messages.[74] The debate over government acquisition of Western Union continued for years and finally ended when Jay Gould died in 1892;[75] by then, the public's reliance on telegraphy was being replaced by a new technology—the telephone.[76]

---

[63] *See* VA. CODE ANN. § 2900 (Michie 1900):

> [T]elegraph companies shall be liable for special damages occasioned in . . . delivering dispatches, or for the disclosure of the contents of any private dispatch to any person other than to him to whom it was addressed, the amount of these damages to be determined by the jury upon the facts in each case. Grief and mental anguish occasioned to the plaintiff may be considered by the jury in the determination of the quantum of damages.

(quoted in Connelly v. W. Union Tel. Co., 40 S.E. 618, 622 (Va. 1902)); *see also* IND. REV. STAT. § 5513 (1894) (cited in W. Union Tel. Co. v. Bierhaus, 36 N.E. 161, 162 (Ind. Ct. App. 1894)).

[64] *See* SMITH, *supra* note 50, at 68.

[65] *Id.* at 68-69; *see also* ERNEST J. EBERLING, CONGRESSIONAL INVESTIGATIONS: A STUDY OF THE ORIGIN AND DEVELOPMENT OF THE POWER OF CONGRESS TO INVESTIGATE AND PUNISH FOR CONTEMPT 231-46 (1928). *See generally* United States v. Babcock, 24 F. Cas. 908 (C.C. Mo. 1876) (ruling on Orton's motion to vacate subpoena requiring production of the telegrams).

[66] SMITH, *supra* note 50, at 69.

---

[67] *Id.*

[68] *Id.* A Kentucky Congressman said Garfield had a "'newfangled sentimentality'" about the confidentiality of telegrams. *Id.*

[69] *Id.*

[70] *Id.*

[71] *Id.* at 70.

[72] *Id.*

[73] *Id.*

[74] *Id.* at 70-71.

[75] *Id.* at 71.

[76] Ronnie J. Phillips, *Digital Technology and Institutional Change from the Gilded Age to Modern Times: The Impact of the Telegraph and the Internet*, 34 J. OF ECON. ISSUES 267, 276-77 (2000), at http://diglib.lib.utk.edu/utj/jei/34/jei-34-2-

When Gould died, the Bell Telephone Company had been in existence for fifteen years.[77] "Boston and New York were talking to Chicago, Milwaukee, Pittsburg, and Washington. One-half of the people of the United States were within talking distance of each other."[78] It had been transmitting a million messages a day since 1888, install its first million telephones in 1898, and would string its first million miles of wire in 1900.[79] "A new generation had grown up, without the prejudices of its fathers. People had grown away from the telegraphic habit of thought, which was that wire communications were expensive luxuries for the few."[80]

---

3.pdf (last visited Aug. 2005).

> It was a competing technology that ultimately destroyed the Western Union monopoly. With the greatly increased demand for the telegraph in the period after the Civil War, the search began for the creation of a "harmonic telegraph" that would enable the simultaneous transmission of multiple messages. In the 1890s, Alexander Graham Bell was teaching deaf mutes in Boston. Two local wealthy businessmen, who each had a deaf child, were impressed by Bell's personality and decided to back him in the race to beat Western Union in the development of a practical harmonic telegraph. While working on the harmonic telegraph, Bell discovered by accident the principles of the telephone. The new technology was demonstrated at the Centennial Exposition of 1876 in Philadelphia.
>
> After a patent dispute with Bell Telephone, in November 1879 Western Union formally contracted to relinquish the rights to the new telephone technology to Bell, under the assumption that the new technology would not challenge the telegraph. Bell Telephone, formed in May 1877, was an immediate success. . . . [W]ithin three years there were 30,000 phones in use around the world. In 1886, there were more than 250,000 phones in use worldwide. By the turn of the century, the telegraph had seen its heyday.

*Id.*

[77] *See supra* note 76.

[78] HERBERT N. CASSON, THE HISTORY OF THE TELEPHONE 183 (1910); *see also supra* note 76.

[79] CASSON, *supra* note 78, at 182.

[80] *Id.* at 178; *see also* JOHN W. OLIVER, HISTORY OF AMERICAN TECHNOLOGY 440 (1956) ("The telephone, unlike the telegraph . . ., was the instrument of, and for, the people. It served individuals of limited means as efficiently as the man of wealth.").

### 3. Telephony

Telephones were less expensive to use than telegraphy, and they held out the possibility of providing more confidentiality because one could communicate directly, instead of relying on telegraph agents to code, transmit, and de-code the contents of the communication.[81] However, the early telephone system was not actually secure because it was not a truly automated system:

> One "party line" would serve four or more customers. Simply by picking up the telephone, . . . customers could hear the conversation of another if the line were in use. . . . [T]his was common because a party-line customer would have no other way of knowing whether the line was free . . . except to pick up the phone and listen. There was no dial tone in those days; . . . operators would direct the call manually at a switchboard. In small towns, you could simply ask the operator for the name of the person you wanted to reach. . . . If the operator had . . . tried to place a call to the same person and gotten no answer, she might tell the caller that the person wasn't home . . . [O]perators knew who was talking with whom, if not the content of the conversation.[82]

---

[81] *See supra* note 60 and accompanying text.

[82] SMITH, *supra* note 50, at 155; *see also* John Bray, THE COMMUNICATIONS MIRACLE: THE TELECOMMUNICATION PIONEERS FROM MORSE TO THE INFORMATION SUPERHIGHWAY 56 (1995):

> The problem of connecting a calling to a called customer was at first solved by manually operated telephone exchanges in which an operator simply plugged in a cord between the corresponding incoming and outgoing telephone line terminals on a switchboard. This system had the advantage that it provided, from the customer viewpoint, good service since the operator could, in systems with small numbers of lines, readily find the called customer by name, and answer queries made by the caller. But it became cumbersome when large numbers of lines were involved, a difficulty only partially solved by the use of 'multiple' switchboards with groups of operators. And there was the inherent problem of 'overhearing' the customers' telephone conversations by the operators and the consequent lack of privacy.

*Id.*

The lack of privacy led a Kansas City undertaker named Almon Strowger to invent an "automatic telephone switching system that dispensed with operators."[83] Strowger patented his device in 1882; it was implemented in Indiana in 1892 and by 1918 it had become the norm for automatic exchanges in the United Kingdom.[84] The Bell system was much slower to adopt automated switching,[85] but by the 1920's it had substantially replaced the operator-assisted system, at least in urban areas.[86]

Once automated switching was introduced, "Americans became comfortable using the telephone for personal and sensitive matters"[87] because they assumed their telephone conversations were confidential or "private." This was, however, an unresolved issue because the introduction of automated switching eliminated operator involvement and essentially resolved the "insider" problem, i.e., the concern that telephone employees would listen in on conversations[88] but it left the "outsider" problem. The outsider problem was the possibility that persons not associated with the telephone company would listen in on what the parties believed to be "private" telephone conversations.

---

[83] BRAY, *supra* note 82, at 57. "Strowger found that he was losing money in his undertaking business because one of the switchboard operators at the Kansas City telephone exchange was married to a rival undertaker and she would connect Strowger's callers wishing to make funeral arrangements to her husband." *Id.*

[84] *Id.* at 59.

[85] *Id.* One reason was a concern that automated switching could not efficiently handle the volume of phone traffic in large cities. *See, e.g.,* Joan Nix & David Gabel, *The Introduction of Automatic Switching into the Bell System: Market versus Institutional Influences,* 30 J. OF ECON. ISSUES 737, 744 (1996).

> Another belief that shaped AT&T's behavior toward automatic switching is related to the perception of the proper role of customers in placing a call. Despite an abundance of information that customers preferred to dial on their own, a consensus was reached that in selecting technology, equipment should be selected that did not require customers 'to do part of the service.' . . . . AT&T's management believed that keeping customer involvement to a minimum would enhance the popularity of telephony. . . . [T]he management of AT&T held on to the ideological presupposition that customers possessed limited capabilities for comprehending the steps involved in dialing a phone.

*Id.* (footnotes omitted).

[86] *Id.*; *see also* Richard R. John, *The Politics of Innovation,* 127.4 DAEDALUS 187, 206 (1998) ("Not until the 1920s, with the widespread introduction of the dial telephone, would Bell democratize telephony by permitting subscribers to hold a telephone conversation without having to rely on . . . operators to make the connection.").

[87] SMITH, *supra* note 50, at 156.

This possibility was not unique to telephonic communication. Technology that could be used to tap telegraphic communications emerged soon after the invention of the telegraph.[89] During the Civil War, the Union and Confederate armies tapped each other's telegraphic communications to obtain information about battle plans and troop movements and after the war rival newspapers tapped each other's wire communications in an effort to be the first to report major stories.[90] Some states had enacted laws making it a crime to intercept telegraphic communications,[91] but there was no federa legislation on point.[92] It is possible that because law enforcement did

---

[88] *Id.* That, of course, was not possible with telegraphy.

[89] Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1270 (2004).

[90] *Id.* (quoting PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 111 (1995)). "Interception of telegrams [during the Civil war] was such a threat that the Union army began using cipher codes to encrypt messages; only generals and the War Department possessed the codes." Thomas F. O'Neill III, Kevin P. Gallagher & Jonathon L. Nevett, *Detours On The Information Superhighway: The Erosion Of Evidentiary Privileges In Cyberspace And Beyond*, 1997 STAN. TECH. L. REV. 3, 4 (1997).

[91] *See* SMITH, *supra* note 50, at 157. *See, e.g.,* 1862 CAL. STAT. 288 (cited in Andrew Ayers, Note, *The Police Can Do What? Making Local Governmental Entities Pay For Unauthorized Wiretapping,* 19 N.Y.L. SCH. J. HUM. RTS. 651, 657 n.63 (2003)).

[92] *See* SMITH, *supra* note 50, at 157. *See, e.g., Ex parte Brown*, 1880 WL 4234 at *5 ("Telegraphic messages are not privileged communications. . . . No statute of this State, or of the United States, has made them so."). There seems to have been little effort to apply *Jackson*'s Fourth Amendment standard to telegrams. In *Brown,* the petitioner apparently did argue for this, contending that "the letter and telegram, so far as the incidents of transmission are concerned, should stand upon the same basis. . . . That the government sends the letter, and a private corporation the telegram, does not affect the principle." *Brown*, 1880 WL at *4. The court disagreed:

> That mode of communication is of recent origin, and, therefore, the com-

not appear to have used wiretaps when investigating crimes,[93] this was not a topic of hot dispute for the public as of yet.

For whatever reason, law enforcement approached the telephone differently: Police had begun to tap telephone conversations at least by the 1890's.[94] The practice, which was not encompassed by state laws outlawing the interception of telegraphic communications, continued for years, becoming the focus of a controversy in 1916. The New York City Police were found to have intercepted telephone conversations with the assistance of the telephone company.[95] The police contended there was no impropriety given the realities of the then-prevalent operator-assisted telephone system: "Telephone conversations . . . cannot be private in the way that letters can be, since the employees of the telephone company cannot help hearing parts of conversations and may, if they are inclined, easily hear all."[96] During this era, there was no telephonic

---

> mon law furnishes nothing but analogies for our guide. Telegraphic lines are not operated by the government . . . . On the other hand postal facilities were established by Congress; the mails are carried by the government through its own agents, and penal statutes protect communications sent through the mail. The entire postal system is under the control and management of the government. . . . There is no such analogy between the transmission of communications by mail, and their tranmission by telegraph, as would justify the application to the latter of the principles which obtain with respect to the former.

*Id.* at *5; *see also* Martin v. Sheriff, 1894 WL 1440 (Ohio Prob. 1894) ("It is not a crime, under the laws of Ohio, to tap a telegraph wire."). There were, however, occasional references to the use of warrants to obtain telegraphic messages.

[93] This may have been due to the fact that "original drafts of telegrams filed with clerks for dispatch, as well as the telegraph company's copies of the received messages, had to be produced for court trials and legislative investigations." John D. Woodward, *Biometric Scanning, Law & Policy: Identifying The Concerns-Drafting The Biometric Blueprint*, 59 U. PITT. L. REV. 97, 119 n.177 (1997) (citing ALAN F. WESTIN, PRIVACY AND FREEDOM 337 (1st ed. 1967)).

[94] *See, e.g.*, Ayers, *The Police Can Do What?*, *supra* note 91, at 658 (in the early 1890's, New York police were the first to tap telephones) (citing WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 155 (1998)). Telephone tapping apparently began much earlier: "In 1881, only five years after the invention of the telephone, a patent was issued for a scrambler that thwarted telephone tappers." *Id.* at 657.

[95] *Id.* (citing SAMUEL DASH ET AL., THE EAVESDROPPERS 25 (1959)).

[96] *Police Espionage in a Democracy*, OUTLOOK 235 (May 31, 1916) (quoted in

analogue of the sealed envelope.[97]

In the 1920's, the implementation of automated switching gave rise to the perception that telephone conversations were private, just as sealed mail was private.[98] This led to greater use of telephones by the public, and by those engaged in unlawful activities; this, in turn, resulted in the Supreme Court's considering whether the Fourth Amendment constrained police wiretapping.[99] The issue in *Olmstead v. United States* was

---

SMITH, *supra* note 50, at 157).

[97] See *supra* note 55 and accompanying text.

[98] See *supra* note 86 and accompanying text.

[99] Prior to Olmstead, only a few reported decisions addressed wiretapping, mostly in the context of prosecutions under statutes that made it a crime to intercept telegraph or telephone messages. *See, e.g.,* State v. Behringer, 172 P. 660, 619 (Ariz. 1918) (holding it was not a violation of Arizona Penal Code section 692—which made it unlawful "by means of any machine, instrument or contrivance" to read or attempt to read "any message, or to learn the contents thereof, whilst the same is being sent over any telegraph or telephone line"—to place a dictograph over the transom of a room and thereby hear what was said over a telephone); *see also Olmstead*, 277 U.S. at 479 n.13 (Brandeis, J., dissenting) (listing statutes that made it a crime to intercept telephone or telegraph messages).

Police wiretapping seems to have been idiosyncratic. *See* Orin S. Kerr, *The Fourth Amendment And New Technologies: Constitutional Myths And The Case For Caution*, 102 MICH. L. REV. 801, 841 n.229 (2004) ("[I]t appears that some state police agencies wiretapped defendants, but others did not."). *See, e.g.,* People v. Hebberd, 96 Misc. 617, 162 N.Y.S. 80 (N.Y. Sup. Ct. 1916). In *State v. Nordskog*, 136 P. 694 (Wash. 1913), the Washington Supreme Court reversed the conviction of a former detective and "professional wire tapper" for "damaging" a telephone line. The court based the conviction solely on his having tapped the line to intercept a message. *See id.* at 694-95. It found that the mere act of tapping the line inflicted no damage, but it also noted the need for legislation to prevent further such acts:

> [T]here has been altogether too much of this form of pilfering going on in this state, and the omission of the law now disclosed calls aloud for legislative action . . . . [T]he law should be so framed that the privacy of all citizens . . . may be protected, and that any tampering or interference, however slight, that is not done under the rules of the company and by its agents, or under some regulation of the public service commission, may be prohibited.

*Id.* at 695; *see also* Robilio v. United States, 291 F. 975, 982-83 (6th Cir. 1923) (upholding the admissibility of evidence obtained by wiretapping the home of the defendant against evidentiary challenges as to its authenticity; no challenge was based on the act of wiretapping itself); People v. McDonald, 165 N.Y.S. 41, 44-45 (N.Y. App. Div. 1917) (refusing to suppress evidence obtained "whether the use of evidence of private telephone conversations . . . intercepted by means of wire tapping, amounted to a violation of the Fourth and Fifth Amendments."[100] Prohibition officers had installed wiretaps on telephone lines leading from the residences of suspected bootlegger Roy Olmstead and three of his associates.[101] The government used the information obtained by the wiretaps to prosecute Olmstead and the others for violating prohibition laws.[102] Since the taps were connected to the telephone lines as they ran toward the residences, there was no physical intrusion into the homes.[103]

---

by tapping the home of the defendant on the grounds that under New York law it was immaterial how the state obtained the evidence and that the Fourth Amendment did not apply to the states, only to the federal government).

[100] 277 U.S. 455 (1928).

[101] Olmstead, a former Seattle police lieutenant, had become the biggest bootlegger in western Washington. *See* W. MURPHY, WIRETAPPING ON TRIAL: A CASE STUDY IN THE JUDICIAL PROCESS 16 (1965); 277 U.S. at 455-56:

> The evidence . . . discloses a conspiracy of amazing magnitude to import, possess, and sell liquor unlawfully. It involved . . . not less than 50 person s, . . . two seagoing vessels for the transportation of liquor . . ., the maintenance of a central office manned with operators, and the employment of executives, salesmen, deliverymen, dispatchers, scouts, bookkeepers, collectors and an attorney. In a bad month sales amounted to $176,000; the aggregate for a year must have exceeded two millions of dollars.

*Id.* Olmstead was the "leading conspirator and the general manager of the business" which utilized telephones in its operations:

> Of the several offices in Seattle, the chief one was in a large office building. In this there were three telephones on three different lines. There were telephones in an office of the manager in his own home, at the homes of his associates, and at other places in the city. Communication was had frequently with Vancouver, British Columbia. Times were fixed for the deliveries of the "stuff" to places along Puget Sound near Seattle . . . . One of the chief men was always on duty at the main office to receive orders by the telephones and to direct their filling by a corps of men stationed in another room . . . . The call numbers of the telephones were given to those known to be likely customers.

*Id.* at 456.

[102] *See id.* at 455 ("The petitioners were convicted in the District Court for the Western District of Washington of a conspiracy to violate the National Prohibition Act . . . by unlawfully possessing, transporting and importing intoxicating liquors and . . . by selling intoxicating liquors").

[103] *See id.* at 456-57:

In an opinion by Chief Justice Taft, a majority of the Court held that the Fourth Amendment[104] did not apply because there was no trespass:[105] "The language of the amendment cannot be . . . expanded to include telephone wires, reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched."[106] Justice Taft was careful to distinguish telephone conversations from letters:

> It is urged that the language of Mr. Justice Field in *Ex parte Jackson* . . . offers an analogy to the interpretation of the

---

> [I]nformation . . . was . . . obtained by intercepting messages on the telephones of the conspirators . . . . Small wires were inserted along the . . . telephone wires from the residences of . . . the petitioners and those leading from the chief office. The insertions were made without trespass upon any property of the defendants. They were made in the basement of the large office building. The taps from house lines were made in the streets near the houses.

[104] The Court found there was no basis for applying the Fifth Amendment because there was "no evidence of compulsion to induce the defendants to talk over their many telephones. They were continually and voluntarily transacting business without knowledge of the interception. Our consideration must be confined to the Fourth Amendment." *Id.* at 462.

[105] *See id.* at 466:

> The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house, and messages while passing over them are not within the protection of the Fourth Amendment. . . .
>
> We think, therefore, that the wire tapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment.

*See id.* at 457 (The taps were installed "without trespass upon any property of the defendants."); *see also id.* at 465 ("'The Fourth Amendment is to be construed in the light of what was deemed an unreasonable search and seizure when it was adopted.'") (quoting Carroll v. United States, 267 U.S. 132, 149 (1925)).

In affirming Olmstead's conviction, the Ninth Circuit explicitly noted the need for a physical trespass: "[The amendment] has never been extended to the exclusion of evidence obtained by listening to the conversation of persons . . . . The purpose . . . is to prevent the invasion of homes and offices and the seizure of incriminating evidence found therein." 19 F.2d 842, 847 (9th Cir. 1927).

[106] *Id.* at 465.

> Fourth Amendment in respect of wire tapping. But the analogy fails. . . . It is plainly within the words of the amendment to say that the unlawful rifling by a government agent of a sealed letter is a search . . . of the sender's papers of effects. The letter is a paper, an effect. . . .[107]

Justice Brandeis famously dissented, arguing that the "Fourth Amendment must adapt to a changing world."[108] He pointed out that when the amendment was adopted, force was

> the only means known to man by which a government could directly effect self-incrimination. . . . It could secure . . . papers and other articles . . . by breaking and entry. . . . But 'time works changes, brings into existence new conditions and purposes.' Subtler and more far-reaching means of invading privacy have become available to the government . . . .The progress of science . . . is not likely to stop with wire tapping. Ways may . . . be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and . . . expose to a jury the most intimate occurrences of the home. . . . Can it be that the Constitution affords no protection against such invasions of individual security?[109]

After *Olmstead*, wiretapping might violate state law, but it was constitutionally permissible; Congress considered banning it, but ultimately did nothing.[110] In 1935, Congress adopted the Federal Communications Act for reasons having nothing to do with *Olmstead*;[111] section 605 of the Act prohibited intercepting a communication without the permission of the sender and divulging or publishing the contents.[112] In 1937, the Supreme Court held that § 605 applied to federal officers, and that evidence obtained in violation of the statute was inadmissible in federal prosecutions.[113] Two years later, it expanded its holding to encompass evidence derived from the use of wiretaps.[114] The Department of Justice took the position that § 605 did not prohibit wiretapping for "purely investigative purposes", and therefore continued to conduct electronic surveillance over the next three decades.[115] During this era, the Supreme Court occasionally heard cases involving the use of wiretaps or other types of surveillance, and always held that, absent a physical trespass, such activity was outside the Fourth Amendment.[116]

---

[107] *Id.* at 464. Justice Taft also held that there was no seizure because the evidence "was secured by the use of the sense of hearing and that only." *Id.*

[108] *Id.* at 474.

[109] *Id.* at 473-74.

[110] *See* Nardone v. United States, 302 U.S. 379, 382 (1937) ("Congressional committees investigated the wire-tapping activities of federal agents. . . . [B]ills were introduced to prohibit the practice, all of which failed to pass.").

[111] *See id.*

In 1967, the Supreme Court reversed *Olmstead* and held that FBI agents violated the Fourth Amendment by installing an "electronic listening and recording device" on the *outside* of a telephone booth to record calls being made by Charles Katz.[117] Katz was convicted of violating section 1084 of the United States Code, which makes it a crime to use facilities of interstate commerce to transmit wagering information.[118]

The conviction was based on six tape recordings, averaging

---

[112] *See* Ch. 652, Title VI, § 605, 48 Stat. 1103 (1934), as amended, 47 U.S.C. § 605.

[113] *See Nardone*, 302 U.S. at 383-84.

[114] *See* Nardone v. United States, 308 U.S. 338, 341-42 (1939).

[115] *See* David S. Eggert, Note, *Executive Order 12,333: An Assessment of the Validity of Warrantless National Security Searches,* 1983 DUKE L.J. 611, 621-22; *see also* Ken Gormley, *One Hundred Years of Privacy,* 1992 WIS. L. REV. 1335, 1362-66.

[116] *See, e.g.,* Goldman v. Unites States, 316 U.S. 129, 135-36 (1942) (declining to overrule *Olmstead*); Goldstein v. United States, 316 U.S. 114, 121-22 (1942) (Fourth Amendment did not apply to wiretapping but evidence obtained in violation of § 605 was inadmissible); *see also* Silverman v. United States, 365 U.S. 505 (1961) (use of spike mike which penetrated party wall and turned heating system serving petitioners' premises into a "conductor of sound" was a trespass and therefore a search under the Fourth Amendment); Irvine v. California, 347 U.S. 128, 131-32 (1954) (police entries into home to install microphone in closet and in a hall was a violation of the Fourth Amendment).

[117] Katz v. United States, 389 U.S. 347, 348 (1967).

[118] *See id.* at 348-49.

> three minutes each, of his end of telephone conversations placed from three public phone booths. The recordings were obtained . . . by means of an electronic listening device attached to the outside of the booths; there was no physical penetration of the . . . booth . . . . . The eavesdropping was conducted only after an investigation indicated that Katz regularly used these phones to call a known gambler. No effort was made, however, to obtain judicial authorization for the eavesdropping.[119]

Katz raised two issues in his appeal, both of which involved the relationship between the Fourth Amendment and a "constitutionally protected area."[120] The Court declined to accept his formulation, explaining that the resolution of "Fourth Amendment problems is not . . . promoted by incantation of the phrase 'constitutionally protected area.'"[121] The majority went on to announce a new Fourth Amendment standard:

> [T]he parties have attached great significance to the . . . telephone booth from which the petitioner placed his calls. The petitioner has . . . argued that the booth was a 'constitutionally protected area.' The Government has maintained . . . that it was not. But this effort . . . deflects attention from the problem presented by this case. For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[122]

---

[119] *Electronic Surveillance*, 82 HARV. L. REV. 187, 187 (1968)

[120] *See* 389 U.S. at 350-51. To this point in history, Fourth Amendment violations occurred only when there was a physical trespass onto a "constitutionally protected area." *See, e.g.,* Erik G. Luna, *Sovereignty and Suspicion,* 48 DUKE L.J. 787, 793 n.20 (1999).

[121] 389 U.S. at 350.

[122] *Id.* at 351 (citations omitted).

The majority then overruled *Olmstead,* explaining that "once it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[123]

In a concurrence, Justice Harlan articulated the standard that has been used to implement the *Katz* holding:[124]

> As the Court's opinion states, "the Fourth Amendment protects people, not places." The question . . . is what protection it affords to those people. . . . My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable." Thus a man's home is, for most purposes, a place where he expects privacy . . . . On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.[125]

It is important to note that Justice Harlan interpreted the majority's opinion as holding "only" (i) that a telephone booth is an area in which one "has a constitutionally protected reasonable expectation of privacy"; (ii) that electronic invasions, as well as physical invasions, of such an area can violate the Fourth Amendment; and (iii) that the invasion of a "constitutionally protected area" without a warrant is presumptively unreasonable.[126] His standard therefore implicitly incorporates the spatially-based conception of privacy that had prevailed since *Olmstead.*[127]

---

[123] *Id.* at 353.

[124] The Court adopted his "reasonable expectation of privacy" standard in *Terry v. Ohio*, 392 U.S. 1, 9 (1968), and has applied it ever since. *See infra* Section I.A.4.

[125] *Id.* at 361 (Harlan, J., concurring).

[126] *Id.* at 360-61.

### 4. Other technology[128]

In *United States v. Knotts*,[129] the Supreme Court applied *Katz* to hold that "the warrantless monitoring of an electronic tracking device ("beeper") inside a container of chemicals did not violate the Fourth Amendment when it revealed no information that could not have been obtained through visual surveillance."[130] The Court found that the information provided by the beeper was nothing more than what the officers could have learned by following the vehicle carrying the container as it traveled to a private cabin:[131]

> A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements . . . . When Petschen travelled . . . he voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final desti-

---

[127] *See supra* note 120. This is evident in his comment that the rule he cites "emerged from prior decisions'"; *supra* note 120 and accompanying text. Those decisions were, by necessity, based on *Olmstead*'s trespass doctrine.

[128] The discussion of Supreme Court cases in this section is selective: It is limited to cases that have dealt with the use of new communicative technologies, as defined in *supra* note 11. The Court has used the *Katz* standard to decide whether a wide variety of police conduct constitutes a "search" under the Fourth Amendment. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 450-51 (1989) (not a search fly over greenhouse in a helicopter and observe marijuana plants through gaps in its roof); California v. Ciraolo, 476 U.S. 207, 213-14 (1986) (not a search for police to fly over backyard in commercial airspace and view marijuana being grown there); Dow Chemical Co. v. United States, 476 U.S. 227, 239 (1986) (not a search to fly over chemical plant and photograph premises). The "technologies" at issue in these cases were simply tools police used to gain a favorable physical vantage point from which to make observations with the unaided, or aided, naked eye; these cases did not involve the type of pervasive, autonomous technologies analyzed in this article. *See infra* Section II.

[129] 460 U.S. 276 (1983).

[130] United States v. Karo, 468 U.S. 705, 707 (1984).

[131] Officers suspected Knotts and others of buying chemicals and using them to manufacture "illicit drugs." *See Knotts*, 460 U.S. at 277-78. They therefore installed the beeper in a can of chemicals and used it to monitor Darryl Petschen as he drove the can to a cabin owned by Knotts. *See id.* at 278-79.

> nation when he exited from public roads onto private property.
>
> . . . Knotts, as the owner of the cabin . . . to which Petschen drove, undoubtedly had the traditional expectation of privacy . . . insofar as the cabin was concerned . . . . But no such expectation of privacy extended to the visual observation of Petschen's automobile arriving on his premises after leaving a public highway.[132]

The Court reached the opposite conclusion in *United States v. Karo*.[133] When DEA agents learned that James Karo and his associates had ordered fifty gallons of ether, the agents concluded that the chemical would be used to manufacture drugs.[134] They arranged to have a beeper installed in one of the cans of ether and used it to track Karo as he drove the cans to his house.[135] On two occasions, they used the signal from the beeper to determine that (i) it was still in Karo's house and (ii) it had been moved to the home of one of his associates.[136] The Supreme Court applied *Katz* to hold that these latter uses violated the Fourth Amendment:

> [P]rivate residences are places in which the individual . . . expects privacy . . . and that expectation is plainly one that society is prepared to recognize as justifiable . . . . In this case, had a DEA agent thought it useful to enter the Taos residence to verify that the ether was actually in the house and had he done so surreptitiously and without a warrant, there is little doubt that he would have engaged in an unreasonable search within the meaning of the Fourth Amendment. For purposes of the Amendment, the result is the same where, without a warrant, the Government surreptitiously employs an electronic device to obtain information that it could not have obtained by observation from outside the curti-

---

[132] *Id.* at 281-82 (citations omitted).

[133] 468 U.S. 705, (1984).

[134] *See id.* at 708-09.

[135] *See id.*

[136] *See id.*

> lage of the house.[137]

The Court reached a similar conclusion in *Kyllo v. United States*,[138] its most recent parsing of the *Katz* standard. The issue in *Kyllo* was whether "the use of a thermal-imaging device aimed at a private home from a public street to detect relative amounts of heat within the home constitutes a 'search' within the meaning of the Fourth Amendment."[139] Federal agents who suspected Danny Kyllo was growing marijuana in his home used a thermal imager to detect heat signatures in his home and garage:

> The scan . . . took only a few minutes and was performed from . . . Agent Elliott's vehicle across the street from the front of the house and also from the street in back of the house. The scan showed that the roof over the garage and a side wall of petitioner's home were relatively hot compared to the rest of the home and substantially warmer than neighboring homes in the triplex. Agent Elliott concluded that petitioner was using halide lights to grow marijuana in his house, which indeed he was.[140]

Indicted for manufacturing marijuana, Kyllo moved to suppress the results of the thermal imaging on the grounds that the scan was a warrantless search conducted in violation of the Fourth Amendment.[141] He eventually pled guilty while reserving the right to pursue this issue on appeal.[142] The Ninth Circuit ultimately rejected Kyllo's argument, holding that he had "shown no subjective expectation of privacy because he had made no attempt to conceal the heat escaping from his home" and that "there was no objectively reasonable expectation of privacy because the imager 'did not expose any intimate details of Kyllo's life,' only 'amorphous "hot spots" on the roof and exterior wall.'"[143]

---

[137] *Id.* at 714-15 (citations omitted).

[138] 533 U.S. 27 (2001).

[139] *Kyllo*, 533 U.S. at 29.

[140] *Id.* at 30.

[141] *See id.* at 30.

[142] *See id.*

The Supreme Court reversed:[144]

> [T]he Fourth Amendment draws "a firm line at the entrance to the house." That line . . . must be not only firm but also bright—which requires clear specification of those methods of surveillance that require a warrant. While it is certainly possible to conclude from the videotape of the thermal imaging that occurred in this case that no "significant" compromise of the homeowner's privacy has occurred, we must take the long view, from the original meaning of the Fourth Amendment forward.
>
> "The Fourth Amendment is to be construed in the light of what was deemed an unreasonable search and seizure when it was adopted, and in a manner which will conserve public interests as well as the interests and rights of individual citizens."
>
> Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a "search" and is presumptively unreasonable without a warrant.[145]

As these cases demonstrate, despite its disavowal of a spatial conception of privacy in *Katz*, the Supreme Court continues to predicate Fourth Amendment privacy upon spatial constraints, that is, upon the occurrence of some type of "intrusion" into a private "place." In *Kyllo* and *Karo*, the "intrusion" is not a physical trespass; it results from the use of technology to extract information that would otherwise be unavailable from a private space. We return to this issue in Section I.C.

---

[143] *Id.* at 31.

[144] *See id.* at 41.

[145] *Id.* at 40 (citations omitted) (quoting Carroll v. United States, 267 U.S. 132, 149 (1925)).

Like Justice Taft, this post-*Olmstead* Court quotes *Carroll v. United States*, 267 U.S. 132, 149 (1925), for the proposition that Fourth Amendment construction is embedded in time, i.e., is based on what was deemed unreasonable when it was adopted. *See supra* note 105. Justice Taft used the quoted passage to buttress his conclusion that wiretapping unaccompanied by physical intrusion into the home was not a violation of the Fourth Amendment. *See supra* note 105. In *Kyllo*, Justice Scalia used it to support his conclusion that technology cannot be utilized as a substitute for physical intrusion. *See Kyllo*, 533 U.S. at 40.

### *B. Third-party records*

> *Recent inventions and business methods call attention to the next step which must be taken . . . for securing to the individual what Judge Cooley calls the right "to be let alone."*[146]

In 1890 Samuel Warren and Louis Brandeis published their famous article, *The Right to Privacy*.[147] Unlike the Fourth Amendment right discussed above,[148] the Warren-Brandeis right (i) was directed at private parties and (ii) did not involve a zero-sum approach to privacy.[149]

Warren and Brandeis were reacting to changes in society and in technology.[150] America was increasingly industrial and urbanized.[151] The urban population provided a market for the new "yellow journalism;" newspapers shifted from political coverage to emphasizing "'sin, sex and violence.'"[152] Advances in photography, such as Eastman's hand-held camera, let amateurs to take "candid" photographs, often clandestinely.[153]

---

[146] Samuel Warren & Louis Brandeis, *The Right to Privacy,* 4 HARV. L. REV. 193 (1890) (quoting THOMAS M. COOLEY, THE LAW OF TORTS 29 (2d ed. 1888)), *available at* http://www.louisville.edu/library/law/brandeis/privacy.html (last visited Aug. 15, 2005).

[147] *See id.*

[148] *See supra* Section I.A.

[149] *See* Warren & Brandeis, *supra* note 146.

[150] *See* Gormley, *supra* note 115, at 1350.

[151] *See id.*

[152] *Id.* at 1351 (quoting EDWIN EMERY & MICHAEL C. EMERY, THE PRESS AND AMERICA: AN INTERPRETATIVE HISTORY OF THE MASS MEDIA 349-50 (3d ed. 1972)).

[153] *See* SMITH, *supra* note 50, at 124. Until 1884, when Eastman invented his hand-held camera, photography "was so cumbersome and the sittings so prolonged that . . . no one's image was captured without their fully knowing it." *Id.* Eastman's invention made it possible, for the first time, for a stranger to photograph someone without their knowledge or permission. *See id.* While we are ac-

These and other forces combined to create a culture in which journalists spied on the socially-prominent,[154] in which individuals had no recourse if their likeness was used for commercial purposes without their knowledge or permission,[155] and in which the use of eavesdropping devices threatened "to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[156]

The Fourth Amendment offered no protection from these activities because it only applies to state action.[157] The "evils" Warren and Brandeis were addressing resulted from the efforts of private citizens, which is why they ultimately cast their right to privacy as a tort: Those whose privacy was violated could bring an "action of tort for damages in all cases" and could seek an injunction "a very limited class of cases."[158] This aspect of the Warren-Brandeis right is relevant to the present discussion because it represents an early attempt to deal with the impact technology has upon "informational privacy," i.e., with an individual's ability to exercise some control over how the private sector gathers, disseminates and uses personal information.[159]

---

customed to this, very few people in the years leading up to Eastman's invention would ever have seen an image of themselves: Mirrors were not common in American households, and only the rich could afford to have portraits painted. *See id.*

[154] *See* Warren & Brandeis, *supra* note 146 ("Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life.").

[155] *See* SMITH, *supra* note 50, at 138.

[156] *See* Warren & Brandeis, *supra* note 146. The concern here is with "private" eavesdropping, rather than with the official activity at issue in *Olmstead.*

[157] *See, e.g.,* Poe v. Ullman, 367 U.S. 497, 549 (1961).

[158] Warren & Brandeis, *supra* note 146 (notes omitted).

[159] *See, e.g.,* Niall Waters, *Personal Privacy and Popular Ubiquitous Technology,* UbiConf 2004 (London), http://www.uclic.ucl.ac.uk/projects/ubiconf/materials/Papers/Niall%20Winters.pdf (last visited Aug. 15, 2005) (informational privacy is the ability of "'individuals, groups or institutions to determine when, how and to what extent information about them is communicated to others'") (quoting ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967)); *see also* Alan F. Westin, *Social and Political Dimensions of Privacy,* 59 J. OF SOCIAL ISSUES 431, 431 (2003) (privacy as "as the claim of an individual to determine what information about himself or herself should be known to others . . . . This, also, involves . . . what uses will

Warren and Brandeis were reacting, as noted earlier, to late nineteenth-century technology: improved printing and photograph reproduction; hand-held cameras; bugs and other eavesdropping devices. These and other technologies transformed personal information into a commodity; the press in prior eras had published information about "notables," but they were usually able to control the information that went to the press.[160] The proliferation of informational technologies and attendant demand for information that arose at the end of the nineteenth century changed all this; the socially- and politically-prominent were obvious targets,[161] but anyone could find that their control over their image or their personal information had been compromised.[162]

Warren and Brandeis faced difficult conceptual difficulties in articulating their new right to informational privacy. One goes to the essence of the principle. The Fourth Amendment assumes a zero-sum conception of privacy in which only two states exist: private or not-private. When Crown officers burst into Entick's home and rummaged through his rooms and boxes, they annihilated the privacy of those spaces; what had been private was now not-private. The conduct with which Warren and Brandeis was concerned was very different; it typically involved capturing and exploiting information that was in the public domain, i.e., photographs and descriptions of the activities of the socially- or politically elite.[163] Since those activities occurred in public—either in public spaces or in homes to which members of the public had been invited—there was no

---

be made of it by others"). *See generally* Gormley, *supra* note 115, at 1350.

[160] *See, e.g.*, MICHAEL SCHUDSON, DISCOVERING THE NEWS: A SOCIAL HISTORY OF AMERICAN NEWSPAPERS 12-57 (1978). *See generally* FREDERICK HUDSON, JOURNALISM IN THE UNITED STATES FROM 1690-1872 (1873).

[161] *See, e.g.*, *id.* at 1352 n.84 (press hounded President Grover Cleveland on his honeymoon).

[162] *See* SMITH, *supra* note 50, at 125, 138-39. Warren and Brandeis have been accused of being elitist, and they were primarily concerned about intrusions into the privacy of the "upper-crust," both because they belong to that society and because members of that society were primary targets for yellow journalists. *See id.* at 135-36.

[163] *See id.* at 121-22.

compromise of information that was secluded, spatially or otherwise from observation. As Warren and Brandeis recognized, what they were concerned about was much more analogous to a property right than to a privacy right; the goal, after all, was to control the collection, dissemination and use of information about an individual.[164]

For various reasons, Warren and Brandeis ultimately chose to style the right for which they argued as a right to privacy, not a property right.[165] As we shall see in Section III, the same issues arise, albeit in different guises, from our experience with late twentieth-century and early twenty-first century technology. Section II reviews some pertinent technologies, and in Section III we consider whether this concern with controlling personal information that has been released into the public domain can be reconciled with Fourth Amendment principles. But first we need to review another strand of Supreme Court doctrine: decisions dealing with the Fourth Amendment's applicability to third-party records.

In the decade after *Katz,* the Supreme Court twice considered whether the Fourth Amendment applies to the government's accessing records generated by, and held by, a third-party, i.e., by someone whom the records concern but who had no role in their creation. In *United States v. Miller,*[166] Miller, who had been indicted on tax charges, moved to suppress records concerning his bank account; federal agents had obtained the records by using a grand jury subpoena, not a warrant.[167] Miller invoked *Boyd,*[168] claiming that the agents had "improperly circumvented" his Fourth Amendment rights.[169] The district court denied the motion; the Fifth Circuit reversed because it found that the government had violated *Boyd*.[170] The Supreme Court disagreed: "We find that there was no intrusion into any area in which respondent had a protected Fourth Amendment interest and that the District Court therefore correctly denied respondent's motion to suppress."[171] This post-*Katz* Court cited a pre-*Katz* opinion for the proposition that

---

[164] *See id.* at 126; *see also* Warren & Brandeis, *supra* note 146 ("[T]he legal doctrines relating to infractions of what is ordinarily termed the common-law right to intellectual and artistic property are, it is believed, but instances and applications of a general right to privacy, which properly understood afford a remedy for the evils under consideration.").

[165] *See id.* at 126; *see also* Warren & Brandeis, *supra* note 146.

[166] 425 U.S. 435 (1976).

[167] *Miller*, 425 U.S. at 437-39.

[168] *See supra* notes 38-39 and accompanying text.

[169] *Id.* at 438-39.

> "no interest legitimately protected by the Fourth Amendment" is implicated by governmental investigative activities unless there is an intrusion into a zone of privacy, into "the security a man relies upon when he places himself or his property within a constitutionally protected area."[172]

The *Miller* Court also noted that "the documents subpoenaed here are not respondent's 'private papers.' Unlike the claimant in *Boyd*, respondent can assert neither ownership nor possession. Instead, these are the business records of the banks."[173]

Three years later, the Court decided *Smith v. Maryland*.[174] *Smith* was the "other half" of *Katz*—the issue was "whether the installation and use of a pen register," which captures the numbers dialed on a telephone, "constitutes a 'search' within the meaning of the Fourth Amendment.[175] After she was robbed, Patricia McDonough began receiving "threatening and obscene phone calls from a man identifying himself as the robber."[176] Police suspicion focused on Michael Lee Smith as the robber, and the

---

[170] *See* United States v. Miller, 500 F.2d 751, 757 (5th Cir. 1974), *reversed* 425 U.S. 435 (1976) ("The venerable *Boyd* doctrine still retains its vitality; the government may not cavalierly circumvent *Boyd*'s precious protection by first requiring a third party bank to copy all of its depositors' personal checks and then, with an improper invocation of legal process, calling upon the bank to allow inspection and reproduction of those copies.").

[171] *Miller*, 425 U.S. at 440.

[172] *Id.* (quoting Hoffa v. United States, 385 U.S. 293, 301-02 (1966)).

[173] *Id.*; *see supra* notes 38-39 and accompanying text.

[174] 442 U.S. 735 (1979).

[175] *Smith*, 442 U.S. at 736.

[176] *Id.* at 737.

> telephone company, at police request, installed a pen register at its central offices to record the numbers dialed from the telephone at [his] home. The police did not get a warrant or court order before having the pen register installed. The register revealed that on March 17 a call was placed from [his] home to McDonough's phone. On the basis of this and other evidence, the police obtained a warrant to search [Smith's] residence. The search revealed that a page in [his] phone book was turned down to the name and number of Patricia McDonough; the phone book was seized.[177]

Arrested and indicted, Smith moved to suppress "'all fruits derived from the pen register'" on the grounds that its installation and use was a warrantless search in violation of the Fourth Amendment.[178] The trial court denied the motion and a divided Maryland Court of Appeals affirmed.[179]

The *Smith* Court began its opinion by reviewing *Katz* and noting that the standard used to implement *Katz* is the two-pronged test Justice Harlan enunciated in his concurring opinion: (i) whether the individual has exhibited a subjective expectation of privacy in the thing, place or endeavor; and (ii) whether society is prepared to regard the individual's subjective expectation of privacy, if any, as reasonable.[180] The Court found that Smith met neither criterion:

> Since the pen register was installed on telephone company property at the telephone company's central offices, petitioner . . . cannot claim that his 'property' was invaded or that police intruded into a 'constitutionally protected area.' Petitioner's claim . . . is that, notwithstanding the absence of a trespass, the State . . . infringed a 'legitimate expectation of privacy' . . . . [A] pen register differs . . . from the listening device employed in *Katz,* for pen registers do not acquire the *contents* of communications. . . .

---

[177] *Id.* (citations omitted).

[178] *Id.*

[179] *Id.*

[180] *Id.* at 740; *see supra* Section I.A.3.

> [P]etitioner's argument that its installation and use constituted a 'search' necessarily rests upon a claim that he had a "'legitimate expectation of privacy' regarding the numbers he dialed on his phone.
>
> [W]e doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize . . . that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. . . . Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.[181]

The Court also (i) rejected Smith's claim that he demonstrated a subjective expectation of privacy by making the calls from his home,[182] and (ii) held that even if he could show such a subjective expectation, it is not one society would regard as reasonable: "[E]ven if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not 'one that society is prepared to recognize as "reasonable."' This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties"[183] The Court cited *Miller* for the last statement.[184]

---

[181] *Id.* at 741-42 (citations omitted).

[182] *See id.* at 743:

> [T]he site of the call is immaterial . . . . Although petitioner's conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed. Regardless of his location, petitioner had to convey that number to the telephone company . . . if he wished to complete his call. The fact that he dialed the number on his home phone rather than on some other phone could make no conceivable difference, nor could any subscriber rationally think that it would.

*Id.*

The Supreme Court has applied the *Miller-Smith* principle in a variety of cases.[185] It summarized the rationale for the principle in *United States v. Jacobsen*:

> [W]hen an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information. Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information . . . .The Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated.[186]

This brings us back to the Warren-Brandeis issue: If, as the Supreme Court indicates, the Fourth Amendment conception of privacy is zero-sum (i.e., private or not-private), how can individuals have any control over the information they (knowingly, unknowingly, willingly, unwillingly) provide to others?

The assumption of risk principle articulated above assumes one has a choice: reveal information and lose privacy or do not reveal information and retain privacy. The Warren-Brandeis article was concerned with disclosures made that were made to other people by chance, i.e., by being in a particular place at a particular time. One could argue that the element of choice is missing, but there is another difficulty with assuming privacy in this context: The complained-of information (photography, description of what someone did) was gathered in an ostentatiously public place—a street, a restaurant, a hotel, etc. It is, after all, inevitable that certain of our actions will occur in public spaces; we cannot insist that our every action is private and must be ignored.

---

[183] *Id.* at 743-44 (quoting Katz v. United States, 389 U.S. 347, 361 (1967) and citing Miller v. Unites States, 425 U.S. 435, 442-44 (1976)).

[184] *See id.*

[185] *See, e.g.,* California v. Greenwood, 486 U.S. 35, 41 (1988); S.E.C. v. Jerry T. O'Brien, Inc., 467 U.S. 735, 735-36 (1984).

[186] 466 U.S. 109, 117 (1984).

The early third-party records cases—*Smith* and *Miller*—go to a different issue. They both concern the privacy of information that was disclosed to a specific party for a specific purpose; the party making the disclosure chooses to reveal the information, but intends that it be a "controlled disclosure." This issue, which was of relatively minor import in the 1970's when *Smith* and *Miller* were decided, becomes extremely important in a world of ubiquitous technology for, as Section II explains, in such a world we interact, necessarily and almost continuously, with systems that gather information, utilize it and share it with other systems. The effect, as Section II explains, is essentially to eliminate private places; Section III considers how this could, and should, impact on the Fourth Amendment principles discussed above.

### C. *Evolution*

*Privacy is a distinctly modern product . . . .*[187]

When we discuss Fourth Amendment privacy, we need to realize first, that it is so far a relatively narrow concept[188] and, second, that the conception of privacy itself is a very recent development.

> In earlier times, individuals were not seen as separate from their families, small communities, or society as a whole. Rath-

---

[187] E.L. Godkin, The *Rights of the Citizen IV—To His Own Reputation*, 8 SCRIBNER'S MAG., July, 1890, at 58 *available at* http://cdl.library.cornell.edu/cgibin/moa/pageviewer?frames=1&cite=http%3A%2F%2Fcdl.library.cornell.edu%2Fcgibin%2Fmoa%2Fmoa-cgi%3Fnotisid%3DAFR7379-0008-7&coll=moa&view=50&root=%2Fmoa%2Fscri%2Fscri0008%2F&tif=00072.TIF&pagenum=65.

[188] *See supra* §§ I(A)-(B).

> er, they were a part of their tribe or social group, and they lived in an environment where people spent much of their time living closely together or under the watchful eye of others in their family or community. Also, they spent little time alone or thinking private thoughts that might question the communal practices and pressure for conformity in the community.[189]

New England colonies had laws prohibiting people from living alone and "forbade construction of homes beyond half a mile from the meeting house, the center of town. This was . . . the layout of the villages in England that the settlers had left."[190] People, even travelers, shared beds and many colonial homes had "no ceilings, so sounds could easily be heard from room to room and anybody willing to climb to the roof beams could peer into another room."[191] "[I]in the early 1800s as the population expanded and city life increasingly closed in on the rural and small village communities, there were increased glimmerings of dissatisfaction" and desires for more privacy.[192] These desires prompted the nineteenth-century Supreme Court decisions discussed in Section I.A. and the Warren-Brandeis effort to establish a "civil" right to privacy.[193] Our interest in, and desire for, privacy increased in the twentieth century, for a variety of reasons.[194] That interest seems to have reached new levels in the early years of the twenty-first century, given our need to accommodate privacy with the realities of the technology discussed in the next section.

---

[189] GINI GRAHAM SCOTT, MIND YOUR OWN BUSINESS: THE BATTLE FOR PERSONAL PRIVACY 24 (1995).

[190] SMITH, *supra* note 50, at 10, 17.

[191] *Id.* at 19-20.

[192] SCOTT, *supra* note 189, at 34.

[193] *See supra* Section I.B.

[194] *See* SCOTT, *supra* note 189, at 50:

> [F]rom the 1850s through the 1950s, a new concern with the right to privacy emerged, because in an increasingly complex, urbanized, multicultural society, there were more and more ways in which one's privacy might be invaded by others—from the government to the press and advertisers to other citizens. At the same time, there were fewer informal community ways to deal with these problems. . . .

*Id.* The expansion of surveillance technology during and after World War II created increased concerns about a loss of privacy.

The Twentieth-century world is vastly different from the Eighteenth-century realities that produced the Fourth Amendment. If we are to preserve its spirit—the desire to maintain an equitable balance between the personal lives of individuals and the needs of law enforcement—we cannot rely on the letter of the law as it existed when the Fourth Amendment was adopted. We must be flexible and forward-looking. We cannot rely solely on what has been, because what will be, has never been.

---

> By the 1950s, the technology that enabled government surveillance had grown by exponential leaps. Parabolic microphones, transmitters the size of cigarette packs, induction-coil devices and miniature television transmitters made it possible for government agents, police, private investigators and average citizen snoopers to watch, listen and record virtually any sound or movement. Accompanying this perfection in technology came the growing use of private detectives as surreptitious information-gatherers in business and family disputes . . . . Attempts by the states to . . . prohibit wiretapping were . . . ineffective. The state statutes tended to create broad exceptions for police conducting eavesdropping . . . . [T]he language of the statutes was rarely drafted to keep up with the swiftly-changing technology, rendering them quickly obsolete. By the time the United States entered the 1960s, most of the attempts to protect individual privacy by curbing electronic surveillance at the state level had failed.
>
> The 1960s soon witnessed a national uproar over the unchecked ability of government and private investigators to eavesdrop . . . . Influential scholars . . . produced volumes of literature detailing the threat of surveillance technology to individual privacy. Newspapers and periodicals . . . featured articles . . . decrying the runaway use of electronic surveillance . . . .

Gormley, *supra* note 115, at 1363-64 (citations omitted). And in his State of the Union address in 1967, President Johnson declared, "We should protect what Justice Brandeis called the 'right most valued by civilized men'—the right to privacy." *Id.* at 1364 (quoting *Text of Message by President Johnson to Congress on State of the Union*, N.Y. TIMES, Jan. 11, 1967, at A16).

## II. TECHNOLOGY

*"Ubiquitous technology/computing will permeate all aspects of our physical world . . . ."*[195]

*Olmstead* and *Katz* were products of the same nineteenth-century technology: the telephone.[196] The Warren-Brandeis right to privacy was the product of other nineteenth-century technologies: improved printing, mobile photography and private surveillance techniques.[197] At the beginning of the twenty-first century, we occupy an environment that has been changed dramatically by twentieth century technologies; telephone booths like the one Charles Katz used are an endangered species,[198] as is the one-to-one mode of communication he utilized. Our communications are multi-modal; we communicate synchronously or asynchronously by voice, text or data, and combine modes.[199] As everything about our lives becomes

---

[195] UbiCorp: A Vision of the Ubiquitous Corporation, Accenture, at http://www.accenture.com/xd/xd.asp?it=enweb&xd=services%5Ctechnology%5Ctech_ubicorp.xml (last visited Aug. 15, 2005).

[196] *See supra* Section I.A.3.

[197] *See supra* Section I.B.

[198] *See, e.g.*, Archive of Addresses by Andy Rooney, Andy Rooney's Phone Dilemma (Jan. 9, 2005), http://www.cbsnews.com/stories/2005/01/07/60minutes/rooney/main665523.shtml ("The public telephone booths that used to be on every big city street corner are rapidly disappearing."). *See also* Oliver Lucazeau, *Last Call for Britain's Little Red Telephone Booths*, THE GLOBE & MAIL (Toronto) June 21, 2004, at A11 (explaining the gradual disappearance of red telephone booths in Britain).

[199] *See, e.g.*, *Highlight of the Month: The Ultimate VAS Environment*, COMVERSE ANALYST NEWSLETTER (Comverse, New York, N.Y.), December 2002, http://www.comverse.com/news/newssub/NEWSLETTER7.htm#What's%20New:

> "Total communication" creates a borderless environment where people are free to communicate in the way that is most appropriate . . . for them. It encompasses the full range of real-time and non-real-time multimedia communications and messaging services. As a result, talking, voice messaging, emailing, text messaging, chatting and conferencing become equally accessible options.

*Id.*; *see also* Posting of Angus Davis to Om Malik's Blog-About the Next Generation Internet, http://gigaom.com/2004/11/29/building-the-phone-platform/ (Nov. 29, 2004) ("IP-powered telecommunications will . . . chang[e] the way people . . . use the more portable, more exposed to scrutiny, we will have to decide how to reconcile the inherent tension between privacy and the need for effective law enforcement.

A relatively recent Ninth Circuit case illustrates how far we have come from *Katz*; *In re the Application of the U.S. for an Order Authorizing the Roving Interception of Oral Communications*[200] arose from the Federal Bureau of Investigation's (FBI) efforts to wiretap a vehicle. More precisely, it resulted from the FBI's efforts to use technology already integrated into a private vehicle to intercept conversations taking place within it.[201] As the Ninth Circuit explained, some vehicles are equipped with "telecommunication devices" that assist with navigation or with "emergencies or obtaining road-side assistance. Such systems operate via a combination of GPS . . . and cellular technology."[202] The appellant in the case (the Company) operated one such service (the System).[203] One feature of the System [let] the Company open a cellular connection to a vehicle and listen to [conversations in] the car."[204] The purpose was to help recover stolen vehicles, but it could also be used to eavesdrop on legitimate conversations carried on in a vehicle equipped with the System.[205]

Realizing this, the FBI obtained "orders requiring the Company to assist in intercepting conversations taking place in a car equipped with the System."[206] The Company complied with the first order but challenged the next, claiming that the district court did not have authority to order the use of its

---

telephone. . . .[T]he two-party voice calling will shift towards multimodal and multi-party communication[s]. . . .").

[200] 349 F.3d 1132 (9th Cir. 2003).

[201] *Id.* at 1134. Law enforcement installation of listening devices in vehicles is far from novel. *See, e.g.*, Massiah v. United States, 377 U.S. 201, 202-03 (1964) (in 1959, federal agents "install[ed] a Schmidt radio transmitter under the front seat of [a car]" and used it to listen in on conversations held by the occupants of the vehicle).

[202] *In re* The Application of the U.S. for an Order Authorizing the Roving Interception of Oral Communications, 349 F.3d at 1133.

[203] *Id.*

[204] *Id.*

[205] *Id.* at 1133-34.

[206] *Id.* at 1134.

"equipment, facilities, system, and employees."[207] The district court rejected the challenge and the Company appealed.[208]

The orders were issued under the federal wiretap statutes: Title III.[209] Congress responded to the *Katz* decision by adopting Title III of the Omnibus Crime Control and Safe Streets Act of 1968;[210] Title III was intended "to implement a uniform procedure for conducting constitutionally acceptable electronic surveillance."[211] Since it is founded upon the Fourth Amendment, Title III makes it illegal to intercept communications except pursuant to a court order.[212] In issuing a Title III order, a court can require "a provider . . . of wire or electronic communication service, landlord, custodian or other person" to provide "technical assistance necessary to accomplish the interception . . . with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted."[213]

The Company claimed it was not a "provider of communication service" under Title III.[214] The Ninth Circuit found it was subject to Title III either as a provider of communications services or as an "other person" who could be required to assist law enforcement in intercepting communications.[215] The Ninth Circuit reversed the district court, however, because it concluded that the surveillance could not be carried out "with a minimum of interference with the services" the Company provided the owner of the vehicle.[216] The court found that "eavesdropping is not performed with 'a minimum of interference' if a service is *completely* shut down as a result of the surveillance."[217] Since officers using the System to eavesdrop shut down its emergency and other functions, the Ninth Circuit held that the district court erred in ordering the Company to cooperate with the FBI.[218]

---

[207] *Id.* at 1134-35.

[208] *Id.* at 1135.

[209] *Id.* at 1136-38.

[210] *See* Title III, Pub. L. No. 90-351, § 802, 82 Stat. 197, 212 (1998); *see also supra* Section I.A.3. Congress was specifically responding to *Berger v. New York*, 388 U.S. 41 (1967). In *Berger,* a companion to *Katz,* the Court held that because of the potential for intrusiveness, wiretapping authorizations must be carefully crafted to satisfy the probable cause and particularity requirements of the Fourth Amendment. *Id.* at 55-64.

[211] Jie Xiu, Note, *The Roles Of The Judiciary In Examining And Supervising The Changing Laws Of Electronic Surveillance,* 28 SETON HALL LEGIS. J. 229, 233 (2003).

[212] *Id.*

[213] 18 U.S.C. § 2518(4) (2000).

[214] *In re The Application of the U.S.*, 349 F.3d at 1139.

[215] *Id.*

This case highlights issues we will face as technology becomes an increasingly pervasive feature of our lives.[219] We have for many decades assumed that a vehicle is a "private" place; fictional characters often take advantage of the privacy a vehicle offers to discuss sensitive matters.[220] The privacy of vehicles has, of course, been compromised on occasion;[221] but while we might be aware, at some level, that cars *could* be "bugged," we could not imagine that our vehicles would themselves *become* instruments of surveillance.

---

[216] *Id.* at 1144-46; *see also* 18 U.S.C. § 2518(4).

[217] *Id.* at 1145 (quoting 18 U.S.C. § 2518(4)).

[218] *Id.* at 1146. A California legislator responded to this decision by introducing Senate Bill 1330, which would prohibit "eavesdropping involving an embedded automotive telematic device." *See* Committee Report for 2003 California Senate Bill No. 1330, 2003-04 Regular Session (July 12, 2004) [hereinafter Committee Report]; *see also* California Senate Bill 1330, as amended June 30, 2004. After the Department of Justice expressed concern that the original bill would preclude "law enforcement agencies from applying for an order authorizing interception of electronic cellular telephone communications that occurred by means of a technology such as" the System, the bill was revised so it does not "reduce the ability of law enforcement agencies to apply for a wiretap order." Committee Report, *supra* ("[B]y enacting a series of prohibitions in the invasion of privacy laws . . . without concurrently creating some explicit, though limited, authority in the wiretapping provisions, this bill reduced the scope of the existing wiretap authority."). According to a committee report, it reaffirms

> California's wiretapping law—bugging by law enforcement is prohibited . . . . [R]ecognizing that emerging forms of technology may combine electronic communications capabilities, this bill provides that a cellular telephone, or a similar device, may not be used to overhear confidential communications between persons who are not using some form of communication technology.

*Id.* On July 2, 2004, S.B. 1330 was withdrawn from the Assembly Committee on Appropriations and set for a second reading. On August 9, 2004, it was amended in Assembly. *See* S.B. 1330, http://info.sen.ca.gov/pub/bill/sen/sb_1301-1350/sb_1330_bill_20040809_amended_asm.html. On August 17, a first hearing was set for the bill, but it was canceled at the request of the bill's author. *See* California State Senate, Complete Bill History: S.B. 1330, http://info.sen.ca.gov/pub/bill/sen/sb_1301-1350/sb_1330_bill_20040817_history.html. If it passes, the bill would prohibit intercepting conversations between the occupants of a vehicle. *See* Committee Report for 2003 California Senate Bill No. 1330, *supra*: "California law authorizes the interception of wire, electronic pager, or electronic cellular telephone communications. Unlike federal law, the statutory scheme set forth in Penal Code Section 629.50 et seq. does not authorize intercepting oral communications, commonly referred to as 'bugging.'"

If cars can become instruments of surveillance, what about our homes? The case discussed above illustrates a trend—the pervasiveness of technology[222]—that will find its way into our homes. As computer technology becomes an embedded feature of every aspect of our lives, our homes, too, will come equipped with technology that can be used to eavesdrop on our conversations and track our activities.[223] Like the System, this technology will be included because it has other uses.[224] Efforts are underway to develop "aware homes" that incorporate intel-

---

[219] *See generally,* Centre for Pervasive Computing, http://www.pervasive.dk/ (last visited Aug. 16, 2005).

[220] The Ninth Circuit case discussed above focused exclusively on the specific statutory structure Title III created for the authorization and implementation of wiretaps, so the question of whether the interior of the vehicle was a "private" place was not raised, though it was presumably assumed. *See generally*, *In re* The Application of the U.S., 349 F.3d 1132 (9th Cir. 2003) (showing how the court focused on the statutory structure of Title III).

[221] *See supra* note 201 and accompanying text.

[222] *See, e.g.*, SeachNetworking.Com Definitions, http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci759337,00.html (last visited Aug. 16, 2005):

> Pervasive computing is the trend towards increasingly ubiquitous . . . connected computing devices in the environment, a trend being brought about by a convergence of advanced electronic-and particularly, wireless-technologies and the Internet. Pervasive computing devices are not personal computers as we tend to think of them, but very tiny-even invisible-devices, either mobile or embedded in almost any type of object imaginable, including cars, tools, appliances, clothing and various consumer goods-all communicating through increasingly interconnected networks. According to Dan Russell, director of the User Sciences and Experience Group at IBM's Almaden Research Center, by 2010 computing will have become so naturalized within the environment that people will not even realize that they are using computers. Russell and other researchers expect that in the future *smart* devices all around us will maintain current information about their locations, the contexts in which they are being used, and relevant data about the users.

*Id.*

[223] *See supra* note 222; *see also* Marc Langheinrich, *et al.*, *Living in a Smart*

---

*Environment: Implications for the Coming Ubiquitous Information Society,* 15 TELECOMM. REV. 1 (2005), at http://www.vs.inf.ethz.ch/publ/papers/sktelecom2005.pdf (last visited Aug. 16, 2005):

> By virtue of its very definitions, the vision of ubiquitous computing has the potential to create an invisible and comprehensive surveillance network, covering an unprecedented share of our public and private life: "The old sayings that 'the walls have ear' and if these walls could talk' have become the disturbing reality. The world is filled with all-knowing, all-reporting things' . . . . Today's economic reality—shopping without participating in comprehensive profiling . . . might become an expensive luxury for well-off citizens . . . .

*Id.* (quoting R. Lucky, *Everything Will Be Connected To Everything Else*, Connections, IEEE SPECTRUM (March 1999), at http://www.argreenhouse.com/papers/rlucky/spectrum/connect.shtml (last visited Aug. 16, 2005)).

[224] *See, e.g.,* Mahesh S. Raisinghani, *et al., Ambient Intelligence: Changing Forms of Human-Computer Interaction and their Social Implications,* 5 J. DIGITAL INFO., Issue 4, Art. 271 (Aug. 24, 2004), *available at* http://jodi.ecs.soton.ac.uk/Articles/v05/i04/Raisinghani/ (last visited Aug. 16, 2005):

> A young mother is on her way home, driving . . . with her 8-month old daughter who is sleeping in her child seat on the passenger side of the car. The infant is protected by an intelligent system called SBE 2 against airbag deployment, which could be fatal in the case of an accident. SBE 2 detects when there is a child seat on the passenger seat instead of a person and automatically disables the airbag . . . . Arriving home, a surveillance camera recognizes the young mother, automatically disables the alarm, unlocks the front door as she approaches it and turns on the lights to a level of brightness that the home control system has learned she likes. After dropping off her daughter, the young mother gets ready for grocery shopping. The intelligent refrigerator has studied the family's food consumption over time and knows their preferences as well as what has been consumed since the last time she went shopping. This information has been recorded by an internal tracking system and wireless communication with the intelligent kitchen cabinets. Based on this information, the refrigerator automatically composes a shopping list, retrieves quotations for the items on the list from five different supermarkets in the neighborhood through an Internet link, sends an order to the one with the lowest offer and directs the young mother there. When arriving at the supermarket, the shopping cart has already been filled with the items on her shopping list. Spontaneously, she decides to add three more items to her cart and walks to the check-out. Instead of putting the goods on a belt, the entire cart gets checked out simply by running it past an RFID transponder that detects all items in the cart at once and sends that information to the cash register for processing.

*Id.*

ligent, embedded systems which interact with the occupants and with outside systems.[225] An "aware home" will "be able to recognize the people that live in it, adapt . . . to them [and] learn from their behavior".[226] Similar systems will become features of offices, hotel rooms and other environments.[227]

Pervasive technology raises difficult issues about privacy.[228] Our Fourth Amendment conception of privacy is spatial-

---

[225] *See, e.g.,* Georgia Institute of Technology, The Aware Home, at http://www.cc.gatech.edu/fce/ahri/ (last visited Aug. 24, 2005); Philips Research, *Ambient Intelligence: A New User Experience*, at http://www.research.philips.com/technologies/syst_softw/ami/vision.html; *see also* Mark Ward, *Smart Homes Offer A Helping Hand,* BBC NEWS, May 19, 2004, at http://news.bbc.co.uk/2/hi/technology/3715927.stm (last visited Aug. 16, 2005).

[226] Philips Research, *supra* note 225; *see also supra* note 224.

[227] *See, e.g.,* European Commission, ISTAG: Scenarios for Ambient Intelligence in 2010, 4-7, 2001, at http://www.research.philips.com/technologies/misc/homelab/downloads/evr.19763en.pdf.

[228] *See, e.g.,* Marc Langheinrich, *Privacy by Design—Principles of Privacy-Aware Ubiquitous Systems,* Proceedings of UbiComp 2001 273 (2001), http://www.vs.inf.ethz.ch/publ/papers/privacy-principles.pdf (last visited Aug. 24, 2005):

> What is it that makes ubiquitous computing any different from other computer science domains with respect to privacy? . . . Four properties come to mind:
>
> - UBIQUITY: Ubiquitous computing is everywhere—this is its essence, its explicit goal. Consequently, decisions made in ubiquitous system and artifact design will affect large, if not every part of our lives, from crossing a street to sitting in the living room to entering an office building.
> - INVISIBILITY: Not only should computers be everywhere, we want them to actually disappear from our views. With the ever shrinking form factor of computing and communication devices, this goal seems far from being science fiction. Naturally, we will going to have a hard time in the future deciding at what times we are interacting with (or are under surveillance by) a computing or communication device.
> - SENSING: As computing technology shrinks and processing power increases, so does the abilities of sensors to accurately perceive certain aspects of the environment. Simple temperature, light, or noise sensors have been around for quite some time, but next generation sensors will allow high quality audio and video feeds from cameras and microphones smaller than buttons. Even emotional aspects of our lives, such as stress, fear, or excitement, could then be sensed with high accuracy by sensors embedded in our clothings [sic] or in our environment.
> - MEMORY AMPLIFICATION: Advancements in speech and video processing, combined with the enhanced sensory equipment available soon, make it actually feasible to perceive memory prosthesis, or amplifiers, which can continuously and unobtrusively record every action, utterance and

ly-driven in the sense that it equates privacy with exclusion.[229] The Supreme Court held that Charles Katz had a Fourth Amendment expectation of privacy in his calls because by retreating to a telephone booth, he sought to prevent others from hearing what he said.[230] *Katz* has created an "assumption of risk" standard:[231] My communications and activities are private only insofar as I shield them from observation by others. We consequently tend to associate "privacy" with enclaves such as our homes, our cars, our offices.[232]

The pervasiveness of technology erodes those enclaves. Cell phones have basically eliminated phone booths; vehicles are equipped with surveillance technology; and with wireless networks and cellular communications, much of what goes on in our homes leaks into the public domain. Offices may be somewhat more secure, but much of our work takes place outside our offices. "Road warriors" equipped with the latest in wireless communication conduct business from—and on their way to and from—other offices, other places. The notion of private enclaves as places separate and apart from the world, areas in which our activities and communications are not subject to observation, is disappearing.

---

> movement of ourselves and our surroundings, feeding them into a sophisticated back-end system that uses video and speech processing to allow us browsing and searching through our past.

*Id.*

[229] *See supra* Section I.A.3.

[230] *See supra* Section I.A.3.

[231] *See, e.g.,* Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data,* 6 MICH. TELECOMM. & TECH. L. REV. 61, 71-73 (2000).

[232] In the *Application of the U.S. for an Order Authorizing the Roving Interception of Oral Communications* case, the FBI proceeded under Title III. Since Title III applies only when one has a reasonable expectation of privacy in the communications at issue, the FBI either (i) operated on the assumption that the interior of the vehicle was a "private" enclave requiring a warrant to access or (iii) proceeded under Title III because the agents needed the cooperation of the Company to exploit the System for eavesdropping purposes. *See supra* notes 200-18 and accompanying text.

## III. TWENTY-FIRST CENTURY PRIVACY?

*"You have no privacy. Get over it."*[233]

In effect, we must decide if the Katz Court meant what it said when it held that the Fourth Amendment "protects people, not places."[234] Notwithstanding that holding, the Court has continued to approach Fourth Amendment privacy as if it is nothing more than a spatial concept; what I seclude from others is private, what I fail to shield is not.[235] The question is whether this is inevitable: Can we construe Fourth Amendment privacy in a fashion that is expansive enough to encompass life in a society where physical barriers have little, if any, meaning?[236] If we cannot, we will have little, if any, privacy.

### *A. Dynamics*

---

[233] On the Record: Scott McNealy, SAN FRANCISCO CHRONICLE, Sept. 14, 2003, at http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2003/09/14/BU141353.DTL&type=business (last visited Aug. 18, 2005) (comment from Chairman, President and CEO of Sun Microsystems, Inc.: "The point I was making was someone already has your medical records. Someone has my dental records. Someone has my financial records. Someone knows just about everything about me.").

[234] *See* Katz, *supra* note 124 and accompanying text.

[235] Historically, the only way to shield my activities and personal information from prying eyes was to physically seclude it from observation, e.g., in locked rooms, sealed chests, etc. *See supra* note 28 and accompanying text. This is apparent in *Katz*; the Supreme Court found that Charles Katz had a reasonable expectation of privacy in his phone calls because he secreted himself in a sealed telephone booth, thereby preventing the unaided ear from hearing what was said. *See supra* Section I.A.3. The physical seclusion of communicated information was also the basis for the Court's decision in *Jackson*; the Supreme Court found a Fourth Amendment expectation of privacy in letters that had been sealed to frustrate casual access to their contents. *See supra* Section I.A.1. As we move into a digital world, we necessarily develop different ways to frustrate access to data; encryption is an obvious example. Encryption frustrates access by "obscuring information to make it unreadable without special knowledge." Encryption, Wikipedia, http:// en.wikipedia.org/wiki/Encryption. It is not a physical barrier but it has the same effect, and the same logic: to block undesired access.

[236] *See supra* Section II.

*" . . . replacing . . . Big Brother . . . with a lot of Little Brothers."*[237]

To understand why that is true, we must consider how ubiquitous technology will alter the basic law enforcement dynamic. Jackson, Boyd, Olmstead, Katz and most of the Supreme Court's other Fourth Amendment decisions involved law enforcement's locating the presumptive situs of physical evidence[238] and then taking affirmative steps to find and seize that evidence, a scenario older than general warrants.[239] The scenario has two notable characteristics. First, officers seek evidence of a specific crime which they believe was committed by a specific person; this focus circumscribes the scope of their efforts.[240] Second, officers seek out and collect this evidence from places associated with the suspect.[241] Fourth Amendment analysis has consequently focused on the interaction between the officers and the suspect; the concern has been with controlling the process by which officers intrude into that person's "private" spaces.[242] The procedures we have devised to prevent "unwarranted" intrusions into personal, private spaces—a search warrant supported by probable cause or an exception—all reflect this.[243] Evidence-gathering that does not intrude into such space is outside the Fourth Amendment, at least as far as the object of the search is concerned.[244]

---

[237] *What Is the Matrix? ACLU Seeks Answers on New State-Run Surveillance Program, American Civil Liberties Union*, October 30, 2003, at http://www.aclu.org/Privacy/Privacy.cfm?ID=14257&c=130 (quoting Barry Steinhardt) (last visited Aug. 18, 2005).

[238] The evidence consists of items of tangible or intangible personal property. *See supra* Section II.A. This includes bodily substances. *See, e.g.*, Schmerber v. California, 384 U.S. 757 (1966).

[239] *See supra* notes 20-21 and accompanying text.

[240] *See, e.g.*, WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT Vol. 1, § 1.1(a) (4th ed. 2005).

[241] *See supra* Section I.A. Law enforcement may also seek evidence from those associated with suspects, as well as from suspects; indeed, officers may seek evidence from "civilians," i.e., those who have no involvement in the suspected criminal activity. That does not alter the structure of the dynamic outlined above. In all of these scenarios—law enforcement searches the suspect's premises, the premises belonging to suspect's associate and the "civilian" premises—the inquiry is whether law enforcement violated the privacy of the person or persons whose premises were the object of a search. The focus is on law enforcement officers' actively targeting someone's premises (*Boyd*) or activity (*Katz*) for scrutiny. *See supra* Section II.A. If the officers violate someone's privacy, they can move to suppress the evidence, if any, resulting from the violation or bring a civil rights suit seeking damages for the violation. *See, e.g.*, FED. R. CRIM. P. 41(h); Groh v. Ramirez, 540 U.S. 551, 554-56 (2004).

Now, consider how this dynamic changes in a world of ubiquitous technology. Ambient technology creates an "invisible and comprehensive surveillance network," the constituent parts of which are operated by private entities. As Section II explained, this network effectively eradicates the distinction between "public" and "private" spaces.[245] Information that has historically been secluded behind physical barriers leaks out into the public domain.[246] The data gathered by such a network, along with the data I generate through my online activities, provides a tremendous opportunity for law enforcement.[247] Instead of having to search variously for discrete

---

[242] *See supra* Section I.A.

[243] *See, e.g.*, FED. R. CRIM. P. 41(c)-(e); LAFAVE, *supra* note 240, § 2.2(a). This assumption is also embedded in Title III, the legislative product of *Katz*. *See supra* notes 209-12 and accompanying text. Title III's wiretap provisions specify that the transmission of the contents of communications is not to be interrupted by "interception;" this is simply an application of the *Jackson* principle. *See* 18 U.S.C. §§ 2510-22; *see also supra* Section I.A. Instead of using an adhesive envelope, one relies upon communication systems that, it has heretofore been reasonable to assume, are "closed" to the general public. *See, e.g.*, COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, U.S. DEP'T OF JUST., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS § IV(A) (2002), at http://www.cybercrime.gov/s&smanual2002.htm#_IVA_ (last visited Aug. 19, 2005):

> Since its enactment in 1968 . . . Title III has provided the statutory framework that governs real-time electronic surveillance of the contents of communications. When agents want to wiretap a suspect's phone, "keystroke" a hacker breaking into a computer system, or accept the fruits of wiretapping by a private citizen who has discovered evidence of a crime, the agents first must consider the implications of Title III.
>
> The structure of Title III is surprisingly simple. The statute's drafters assumed that every private communication could be modeled as a two-way connection between two participating parties, such as a telephone call between A and B. At a fundamental level, the statute prohibits a third party (such as the government) who is not a participating party to the communication from intercepting private communications between the parties using an "electronic, mechanical, or other device," unless one of several statutory exceptions applies.

*Id.*; *see* 18 U.S.C. § 2511(34)(b). *See, e.g.*, *Telephone tapping*, Wikipedia, http://en.wikipedia.org/wiki/Wiretap (last visited Aug. 19, 2005).

[244] *See supra* Section II.

[245] *See supra* note 223; *see also* ROBERT D. O'HARROW, JR., NO PLACE TO HIDE

---

291 (2005):

> Before long, our phones, laptop computers, PalmPilots, watches pagers, and much more will play parts in the most efficient surveillance network ever made. Forget dropping a coin into a parking meter or using a pay phone discreetly on the street. Those days are slipping by. The most simple, anonymous transactions are now becoming datapoints on the vast and growing matrix of each of our lives.

*Id.*

[246] *See supra* Section II.

[247] The data gathered by these sources can be divided into three broad categories:

(i) Tool Data

Tool data encompasses personal information that is valued not for its content but for its utility. It includes Social Security numbers, dates of birth, driver's license numbers and other data; it will no doubt come to include biometric identifiers such as DNA. Tool data is a given; it is not the product of my will or effort but is assigned, more or less arbitrarily, to me. Tool data has "value" because it is an implement that can be used for good or evil. My Social Security number, for example, is a tool I can use to identify myself for various benign purposes (positive value) and one a criminal can use to steal my identity (negative value). *See, e.g.,* Bowen v. Roy, 476 U.S. 693, 710-11 (1986).

Though tool data is something I "receive," it is not inherently "public." My Social Security number and date of birth may be "public," in that I have shared them with others, but that is not inevitable, like the other types of tool data in current circulation, they are "public" because we have not conceptualized tool data as a commodity that has "value" and must therefore be protected. The need for, and use of, tool data is a historical accident, an ad hoc solution to the complexity of modern society; we use tool data to identify ("I am Susan Brenner") and authenticate ("Here is proof I am Susan Brenner"). *See, e.g.,* BRUCE SCHNEIER, BEYOND FEAR 182-95 (2003). For most of human history, these functions were relational; people were born, raised and lived their lives in the same community, where everyone knew and recognized them. SCHNEIER, at 184. As populations became increasingly mobile and urbanized, relational identification and authentication no longer sufficed; it became necessary to find some surrogate, and that is what Social Security numbers, driver's licenses and other personal data became. *See, e.g.,* Matt Sundeen, *License to Drive = Proof of Identity,* STATE LEGISLATURES, April, 2003.

(ii) Biographical Data

Biographical data derives from my activities in real- and cyber-space; it includes where I live and where I have lived, where I work and where I have worked, the car I drive, the routines I follow and the places and people I visit. Biographical data is considered "public" because it is the product of my behavior in public places, where what I do can be observed by anyone who shares that space with me. *See* Remsburg v. Docusearch, Inc. 816 A.2d 1001 (N.H. 2003). Consequently, biographical data, defined as information which was or could have been obtained by observing activity in a "public" place, is not private under *Katz* or under cognate tests used to implement civil privacy protections. *See* United States v. Knotts, 460 U.S. 276, 282-85 (1983); *Remsburg*, 816 A.2d at 1009. As Section II explained, the implementation of ubiquitous technology makes the assumptions underlying this category increasingly problematic because it is based on a purely spatial bifurcation of "public" and "private."

### (iii) Transactional Data

Transactional data is generated by our interactions with others. In analyzing the privacy of transactional data, it is useful to divide it into two types: (a) professional transactional data, which results from interactions with attorneys, physicians, religious advisors, psychiatrists, accountants and other professionals; and (b) commercial transactional data, which results from interactions with those who provide commercial goods or services offline or online. There are certain constants across these categories: Each generates data which establishes (i) that I interacted with a particular professional or commercial resource on one or more occasions, (ii) the nature of that interaction (seeking legal advice, making a purchase) and (iii) the details of that interaction (seeking legal advice about an estate; purchasing vitamins, electronics or clothing). None of this data is private under the *Katz* test or cognate civil standards because by interacting with external entities (human or automated) I have knowingly exposed (i)-(iii) to public view; I assumed the risk that those with whom I interact will reveal the details of that interaction to others.

There can be some overlap between transactional data and biographical data. To understand why, it is useful to consider two real world transactions. In the first, I consult with an attorney whose office is in my neighborhood; in the second, I purchase a prescription from a pharmacist at my local drug store. My traveling to the law office and to the drug store takes place in public, and so can be considered biographical data. It is also transactional data insofar as it shows that I interacted with the lawyer and with the pharmacist. These respective encounters differ somewhat in the extent to which the nature and details of the interactions are biographical. My purchasing a prescription from the pharmacist takes place in "public," and so the nature of the transaction tends toward the biographical; but the details of the purchase will remain confidential unless I choose to share them or unless the pharmacist is indiscreet enough to announce the nature and uses of the medication I buy. Since it is reasonable to infer that I went to a law office to obtain legal advice, the nature of that transaction also tends towards the biographical; but since the transaction itself does not take place in public, the details do not constitute biographical data.

The law has treated the categories differently: Professional interactions are usually encompassed by privileges that bar the professional from revealing details of the interaction without the client's permission; the purpose is to provide confidentiality when it is "essential to the full and satisfactory maintenance of the bits of information from a disjointed array of physical sources, officers can harvest information that is held by these private entities.[248] Under current Fourth Amendment principles, I

---

relationship between the parties." PAUL F. ROTHSTEIN & SUSAN W. CRUMP, FEDERAL TESTIMONIAL PRIVILEGES § 1.1 (2004). For commercial interactions, the general rule is that "the facts of a transaction belong jointly and severally to the participants. If Alice buys a chattel from Bob, ordinarily both Alice and Bob are free to disclose this fact." A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1521-22 (2000) (noting that a "very small number of statutes impose limits upon the sharing of private transactional data collected by persons not classed as professionals"). Neither type of transactional data is private in the constitutional-common law sense, but the evidentiary and other constraints American law places on the dissemination of data resulting from professional interactions limit its circulation to those involved in the professional consultation; therefore, while professional transactional data is not private, it is secured.

[248] *See, e.g.*, Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. *2-3 (2003) (LEXIS):

> The Internet was initiated by the State, and soon after was privatized . . . . Market powers . . . facilitated the rise of new players . . . who gained power and control in the information environment . . . . A convergence of interests seems to be developing among players such as copyright owners and service providers on the one hand, and the State's growing interest in the digital environment, on the other hand. Law enforcement agencies seek to enhance their monitoring capacity and online businesses seek to prevent fraud and combat piracy while strengthening their ties with authorities. This convergence might lead to an unholy alliance with potentially troublesome results . . . .
>
> The most explicit example . . . is reflected in a presentation by Joseph E. Sullivan, director of compliance and law enforcement relations at eBay. Addressing law enforcement agents at a conference on cybercrime, Sullivan offered to hand over information, when requested . . . . eBay is one of the largest online e-commerce businesses, and the owner of PayPal, which provides clearing services for online financial transactions. eBay controls access to a colossal amount of information, including financial records, names, user IDs and passwords, affiliations, e-mail addresses, physical addresses, shipping information, contact information, and transaction information (i.e., bidding history, prices paid, feedback rating). But eBay is not alone in implementing law enforcement-friendly policy. The emerging regime of recent years facilitates cooperation between the State and the private sector in law enforcement efforts, beyond the reach of judicial review.

*Id.* (note omitted); *see also* O'HARROW, *supra* note 245, at 300:

> Law enforcement and intelligence services don't need to design their own surveillance systems . . . . They only have to reach out to the companies that already track us so well while promising better service, security, effi-

have no expectation of privacy in information I have shared with these entities or information they have gathered about me.[249] The essential dynamic is missing. The officers are not directing their efforts *at* me and my private spaces; they instead direct their efforts at others in order to obtain information *about* me. The focus shifts from official intrusions into spaces under my temporary or permanent control to the acquisition of evidence from sources over which I exercise no control. I become irrelevant except as the object of the data acquisition.

The harvesting scenario will not supplant the traditional dynamic. We are physical beings and, as such, will continue to act, and to generate physical evidence, in the real world. The primary locus of evidence for traditional crimes such as rape, murder and drug trafficking will no doubt remain in the real world.[250] The "harvesting" scenario instead represents a new,

---

> ciency, and, perhaps most of all, convenience. It takes less and less effort each year to know what each of us is about. When we were at the coffee shop and where we went in our cars. What we wrote online, who we spoke to on the phone, the names of our friends and their friends and all the people they know. When we road the subway, the candidates we supported, the books we read, the drugs we took, what we had for dinner, how we like our sex.
>
> More than ever before, the details about our lives are no longer our own. They belong to the companies that collect them, and the government agencies that buy or demand them in the name of keeping us safe . . . .

*Id.*

[249] *See supra* Section I.B.; *see also supra* note 244. There are a number of federal statutes—such as the Health Insurance Portability and Accountability Act (HIPAA), the Right to Financial Privacy Act, the Gramm-Leech-Bliley Act and the Electronic Communications Privacy Act (ECPA)—which impose restrictions on the dissemination of various types of personal data. *See, e.g.,* 45 C.F.R. § 164.512(e) (HIPAA); 12 U.S.C. § 3405) (Right to Financial Privacy Act); 15 U.S.C. § 6802(e)(8) (Gramm-Leech-Bliley); 18 U.S. Code § 2703 (ECPA). These and similar statutory provisions are not relevant to this discussion (a) because the restrictions they impose are usually less than those required by the Fourth Amendment and (b) they are far more fragile than the Fourth Amendment. *See, e.g.,* Peter P. Swire, *Katz Is Dead, Long Live Katz,* 102 MICH. L. REV. 904, 916 (2004). What Congress gives, Congress can take away. Public awareness is another issue: The average American is unlikely to be aware of the provisions of these statutes (except, perhaps, to the extent that some require one to fill out paperwork), but does have at least a pragmatic grasp of Fourth Amendment guarantees.

[250] Even crimes such as this generate evidentiary data. *See, e.g.,* Eric

added dynamic, a twenty-first century variation of the "assault on the castle" that ultimately resulted in the adoption of the Fourth Amendment.[251] There are commonalities between the two. A concern for the sanctity of personal information runs from *Entick* through *Jackson* and *Boyd,* and is implicit in *Katz* and *Berger.*[252] These cases, however, all involved the traditional Fourth Amendment dynamic: a direct assault upon personal information in the hands of the person to whom it pertains. The issue we must resolve is whether the Fourth Amendment can, and should, be construed as encompassing indirect assaults as well.

We begin with whether it *should* be construed in this fashion.[253] The impetus, if any, for such a construction must lie in the current interpretation's inability to protect us from new and "unwarranted" governmental intrusions. And that brings us back to the new dynamic. The "harvesting" dynamic has

---

Weslander, *Web Evidence Used in Murder Hearing,* Lawrence (Kansas) Journal-World, December 10, 2004, at http://www.ljworld.com/section/crime_fire/story/189998:

> The case of a Kansas State University professor charged with murdering his ex-wife headed into uncharted legal territory Thursday as prosecutors presented evidence of an Internet search history from the suspect's computers.
>
> . . . .
>
> A Lawrence Police detective who examined computers seized from Thomas E. Murray testified that in the month before Carmin D. Ross' killing, Murray's computers had been used to search the Internet for phrases that included 'how to hire an assassin,' 'how to kill someone quickly and quietly' and 'how to murder someone and not get caught.'
>
> . . . . [The detective] testified that even though Murray appeared to use his computer regularly on Thursday mornings, there was virtually no file activity on Murray's computers the morning of Nov. 13, 2003, the day prosecutors allege he drove to Lawrence and stabbed and beat Ross to death.

*Id.*

[251] Wilson v. Layne, 526 U.S. 603, 609-10 (1999); *see supra* Section I.A.

[252] *See supra* note 210; Section I.A. *See, e.g.,* Berger v. New York, 388 U.S. 41, 49 (1967) (citing *Entick* and noting that the "law, though jealous of individual privacy, has not kept pace with . . . advances in scientific knowledge" such as wiretapping).

[253] The issue as to whether we *can* construe the Fourth Amendment in this fashion is examined in Section III.B., *infra.*

troubling implications for our ability to balance the often-conflicting demands of privacy and of effective law enforcement. This is because it supports two types of law enforcement evidence-gathering, both of which are outside the strictures of the Fourth Amendment.[254] The first scenario is the one discussed above, in which officers collect information about me, specifically, from private entities.[255] While it is outside the Fourth Amendment, this scenario is conceptually more analogous to the traditional Fourth Amendment dynamic in that its focus is narrower; the concern is with gathering evidence about a specific person who is suspected of specific criminal activity.[256] The second scenario is based on the same principle as the first, but is broader in scope. Since none of us have a Fourth Amendment expectation of privacy in data held by private entities,[257] it follows that law enforcement should be able to utilize the resources of these entities to harvest information generally, for strategic, as well as investigative, purposes.[258]

---

[254] There are, as noted earlier, statutory restrictions on certain types of information-gathering. *See supra* note 249 and accompanying text.

[255] *See supra* note 248-49 and accompanying text.

[256] *See id.*

[257] *See supra* Section I.B. Again, there are statutory restrictions on certain types of information-gathering. *See supra* note 249 and accompanying text.

[258] *See* Creating a Trusted Information Network for Homeland Security 31, Second Report of the Markle Foundation Task Force, December, 2003, at http://www.markletaskforce.org/reports/TFNS_Report2_Master.pdf:

> Government agencies have always had access to certain kinds of privately held information. But historically, information requests to commercial organizations were made on a case-by-case basis . . . .
>
> With the advent of data-mining and . . . the increasing computational power of computers . . . agencies at all levels of government are now interested in collecting large amounts of data from commercial sources. Such data might be used not only for investigations of specific people . . . but also to perform large-scale data analysis and pattern discovery . . . .

*Id. See, e.g.,* William J. Krouse, The Multi-State Anti-terrorism Information Exchange (MATRIX) Pilot Project 1, Congressional Research Service (2004), http://www.matrix-at.org/CRS_MATRIX_Report.pdf (last visited Aug. 19, 2005) (project intended to let investigators "share and analyze information that is already available to law enforcement from open public and state-owned data, without a subpoena or court order"); *see also id.* at 8:

> [I]n the past decade, the quantity of personal data held by the private sector has exploded, as computing and storage capabilities have rapidly

These scenarios are troubling because they allow law enforcement officers to accomplish indirectly what they may not be able to accomplish directly. Assume, for example, that officers are investigating illegal activity and suspect I am involved in this activity. Historically, the only ways for them to pursue that suspicion were (i) to question my associates (which does not implicate my privacy);[259] (ii) to question me (which raises Fifth Amendment issues);[260] and (iii) to search for physical evidence that was likely to be in my possession and consequently likely to be in "private" areas under my control. The officers cannot pursue option (iii) unless and until they develop probable cause, obtain a search warrant and execute the warrant with the precision it requires.[261]

---

> advanced, and associated costs have correspondingly diminished. The same could be said of public data held by federal, state, and local governments. Much public and private sector data have been aggregated into "data marts." This information is often available commercially for sale from companies specializing in data aggregation, like ChoicePoint, Equifax, Experian, Qsent, LexisNexis, and Westlaw. With advanced computing technologies tera- and petabytes of data can be manipulated, and multiple data marts can be merged or crossreferenced. Moreover, computer applications are available to 'mine' these data for the purposes of profiling, pattern analysis, link analysis, transactional footprinting, and identity verification.

*Id.* (notes omitted). "Link analysis" is "uncovering relationships that may be indicative of suspicious patterns, groups, or connections." *Id.* at n.42. "Transactional footprinting" involves identifying "the data trails of suspicious activities by individuals and groups" from the records of their online activity. *Id.* at n.43. For the evolution of the Matrix Project, *see, e.g.*, ROBERT D. O'HARROW, JR., NO PLACE TO HIDE 98-124 (2005). For another perspective, *see, e.g.*, Creating a Trusted Information Network for Homeland Security 30, Second Report of the Markle Foundation Task Force, December, 2003, at http://www.markletaskforce.org/reports/TFNS_Report2_Master.pdf (last visited Aug. 19, 2005).

[259] *See, e.g.*, Hoffa v. United States, 385 U.S. 293, 302 (1966) ("Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it"); *see also infra* Section III.B.2.

[260] *See, e.g.*, United States v. Mandujano, 425 U.S. 564, 572-73 (1976) (grand jury testimony); Miranda v. Arizona, 384 U.S. 436, 444 (1966) (custodial interrogation).

[261] *See supra* Section I.A. This is true regardless of whether the officers seek evidence in "private" spaces belonging to me, the suspect, or to others who may or may not have been involved in my criminal activity. *See supra* note 240 and

But option (iii) is compelling only insofar as the information the officers need to confirm my involvement in criminal activity is physical evidence located in "private," physical spaces. Assume that the physical evidence (if any) is not the only means of accomplishing this; assume that I exist in a world where the pervasiveness of technology surpasses its current levels. I may live and work in circumscribed physical spaces, but those spaces, as well as my modes of transportation and the implements I use to conduct my routine activities, are all "live," i.e., they all track my activities.[262] It is almost certain that, in such an environment, the officers could find the confirmatory evidence[263] they need indirectly, by consulting the private entities which provide these technologies and, in so doing, incidentally compile information about me.[264] Since I have no Fourth Amendment expectation of privacy in this information, the officers can obtain it without a warrant[265] based on suspi-

---

accompanying text.

[262] *See supra* Section II.

[263] They can do this in either of two ways: First, in an era of cyberlife and cybercrime, digital evidence may be all they need. If that is true, they should be able to obtain what they need from the various service providers, in the form of transactional data and biographical data (records of my comings and goings, etc.). *See supra* note 248 and accompanying text. Second, if the criminal activity necessarily involves physical evidence (drugs, murder, theft of tangible property), the information they obtain from these third-parties should be sufficient, directly or inferentially, to provide the probable cause they need to enter my premises to search for and seize the physical evidence.

[264] *See supra* Section II. There are two ways the officers can gain access to this information: The private entities can provide it voluntarily or, if they decline to do so, officers can obtain process not requiring probable cause (court order, subpoena) to compel the entities to cooperate. *See supra* note 247 and accompanying text.

[265] *See supra* Section I.B.; *see also* California Bankers Ass'n v. Shultz, 416 U.S. 21, 94-95 (1974) (Marshall, J., dissenting):

> By compelling an otherwise unwilling bank to photocopy the checks of its customers, the Government has as much of a hand in seizing those checks as if it had forced a private person to break into the customer's home or office and photocopy the checks there . . . . Our Fourth Amendment jurisprudence should not be so wooden as to ignore the fact that through micro-filming and other techniques of this electronic age, illegal searches and seizures can take place without the brute force characteristic of the general warrants which raised the ire of the Founding Fa-

cion or simple curiosity. That possibility creates the specter of a twenty-first century analogue of the general warrant,[266] an *ad hoc* procedure that would let officers "investigate merely on suspicion that the law is being violated, or . . . because [they want] assurance that it is not."[267]

---

> thers . . . . As we emphasized in *Katz v. United States,* 389 U.S. 347 (1967), the absence of any physical seizure of tangible property does not foreclose Fourth Amendment inquiry . . . . By the same logic, the Fourth Amendment should apply to the recording of checks . . . . And such a massive and indiscriminate search and seizure, not only without a warrant but also without probable cause to believe that any evidence to be obtained is relevant to any investigation, is plainly inconsistent with the principles behind the Amendment . . .

*Id.* (internal citations omitted). Again, there are statutory restrictions on certain types of information-gathering. *See supra* note 247 and accompanying text.

[266] *See supra* notes 19-22 and accompanying text; *see also supra* note 265 and accompanying text. The dangers of this practice were pointed out almost three decades ago. *See* Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission, Chapter 9, 1977, at http://aspe.hhs.gov/datacncl/1977privacy/c9.htm (last visited Aug. 19, 2005):

> Traditionally, the records an individual might keep on his daily activities, financial transactions, or net worth were beyond government reach unless the government could establish probable cause to believe a crime had been committed. If government were merely suspicious and wanted to investigate, such records were unavailable. The legal standards that protected them evolved in a world where such records were almost universally in the actual possession of the individual. Reflecting that reality, the law only barred government from seizing records in the possession of the individual . . . . [T]hat world no longer exists. Third parties . . . now keep a great many records documenting various activities of a particular individual. Indeed, these third parties keep records about the individual he would not ordinarily have kept in the past. Records for life and health insurance, for example, are repositories of highly intimate personal data . . . which were virtually unknown until recent decades . . . .
>
> . . . .
>
> The existence of records about an individual that are not in his possession poses serious privacy protection problems . . . . Record keepers can [and] often do, . . . disclose records . . . to government without seeking the individual's approval . . . . A government request made informally through a personal visit to the record keeper or by a telephone call . . . may leave no trace . . . . Even if the individual is given notice and documentation of the disclosure, he has no legal right to challenge the propriety of government access to his records, despite the possibility that the government agent might have been on a "fishing expedition."

*Id.* (notes omitted).

[267] United States v. Morton Salt Co., 338 U.S. 632, 642-43 (1950) (referring to

Now consider a variation of this hypothetical: Officers are curious about specific illegal activity, either because they have reason to believe it is occurring or because they want assurance that it is not. Since their belief (if any) is not based on articulable facts indicating that the activity is attributable to particular individuals, they cannot utilize the traditional Fourth Amendment dynamic (option (iii)).[268] Instead, they decide to rely on the second scenario available under the new "harvesting" dynamic.[269] They therefore analyze data "harvested" from private entities[270] in an effort to identify transactional or other patterns which inferentially support the conclusion that particular individuals may be engaging in the suspected illegal activity.[271] Some of the data they analyze may pertain to me, but as I have no Fourth Amendment expectation of privacy in that data, I cannot challenge its use.[272] The procedure in this hypothetical is even more analogous to the general warrants the Fourth Amendment was intended to eliminate.[273]

But while the procedures in both hypotheticals—each a variant of the "harvesting" dynamic—are functionally analogous to general warrants, one element is lacking: a violation of

---

grand jury).

[268] *See supra* notes 256-258 and accompanying text.

[269] *See supra* notes 250-255 and accompanying text.

[270] They can do this in any of several ways: (i) ask the relevant private entities to provide them with data sets encompassing the individuals and parameters they wish to explore so they can perform the analysis; (ii) ask the relevant private entities to use their data to perform the analysis; or (iii) use data sets they have already acquired from private entities to perform the analysis. *See supra* note 255. As noted earlier, the officers can obtain the data voluntarily or through the use of non-Fourth Amendment process. *See supra* note 261.

[271] *See supra* note 255.

[272] *See supra* Section I.B. Again, there are statutory restrictions on certain types of information-gathering. *See supra* note 247.

[273] *See supra* note 264 and accompanying text. The purely indiscriminate nature of this procedure makes it more precisely analogous to the writs of assistance which the colonist deeply resented. *See, e.g.,* LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION, *supra* note 4, at 54 (writ of assistance "was good as a continuous license and authority during the whole lifetime of the reigning sovereign" so the "discretion delegated to the official was therefore practically absolute and unlimited").

privacy. Unless we conclude that the data at issue in scenarios such as these is "private," what is hypothesized here can become reality.

### *B. Options*

> *What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection. . . .*[274]

If we decide we should address the "harvesting" dynamic by adopting a more expansive interpretation of the Fourth Amendment,[275] we have to deal with the second issue: How *can* we possibly find that information I have shared with others is private? The notion seems hopelessly contradictory: I tender information to others, thereby surrendering control over it and assuming the risk that the recipients will disseminate it, but insist that it somehow remains "private."[276]

To resolve this issue, we must parse the apparent contradiction. It derives from the "assumption or risk" principle articulated in *Katz*:[277] Something is "private" only as long as I shield it from "public" view.[278] Privacy is therefore an oppositional concept; I must take steps to secure my spaces, my activities, and my communications if I am to claim they are "private."[279] But is it also a zero-sum concept? That is, can I share my spaces, my activities and my communications with (some) others and still legitimately claim they are "private?" Does the Fourth Amendment encompass a concept of "shared privacy"? Or is there no middle ground between "private" and "public?"

We actually have very little guidance on this issue. The

---

[274] Katz v. United States, 389 U.S. 347, 351 (1967).

[275] *See supra* Section III.A.

[276] *See supra* Section I.B.

[277] *See supra* note 274 and accompanying text; *see also* Section II, *supra.*

[278] *See id.*

[279] *See, e.g.*, Susan W. Brenner, *The Privacy Privilege: Law Enforcement, Technology and the Constitution,* 7 U. FLA. J. TECH. L. & POL'Y 124, 168-82 (2002), http://grove.ufl.edu/~techlaw/vol7/issue2/brenner.pdf.

*Katz* Court talked about "public" view, but did not define "public."[280] Inferentially, however, it is clear that I do not forfeit my Fourth Amendment expectation of privacy if I expose my spaces, my activities and my communications to "some" others; the critical distinction seems to be between controlled exposure to those with whom I have a relationship and promiscuous exposure to a generalized public.[281] This distinction is implicit in decisions that have recognized a reasonable expectation of privacy in premises shared by those who have some type of relationship (family, houseguests, roommates).[282] It is clear that I do not surrender my Fourth Amendment expectation of privacy by "knowingly expos[ing]"[283] my spaces, my activities and my communications to those with whom I share a home, for example.[284] As Justice Scalia said in *O'Connor v. Ortega*, "[i]t is privacy that is protected by the Fourth Amendment, not solitude. A man enjoys Fourth Amendment protection in his home . . . even though his wife and children have the run of the place . . . ."[285]

---

[280] *See supra* Section I.A.

[281] *See, e.g.*, Mary I. Coombs, *Shared Privacy and the Fourth Amendment, Or the Rights of Relationships*, 75 CAL. L. REV. 1593, 1618 (1987):

> The exact contours of . . . shared privacies remain to be explored. Clearly, however, where the claimant is part of a sufficiently small and intimate group that shares a place, she has an expectation of privacy there that should be recognized. For example, assume that a husband has sole legal ownership of the family residence. Few would dispute that his wife, or adult child living at home, should be able to challenge a search of that home.

*Id.* (notes omitted).

[282] *See, e.g.*, Minnesota v. Olson, 495 U.S. 91, 96-97 (1990); *see also id.* at 98-99:

> To hold that an overnight guest has a legitimate expectation of privacy in his host's home merely recognizes the everyday expectations of privacy that we all share. Staying overnight in another's home is a longstanding social custom that serves functions recognized as valuable by society. We stay in others' homes when we travel to a strange city for business or pleasure, when we visit our . . . relatives out of town, when we are in between jobs or homes, or when we house-sit for a friend. We will all be hosts and we will all be guests many times in our lives. From either perspective, we think that society recognizes that a houseguest has a legitimate expectation of privacy in his host's home.

*Id.* This notion of shared, relational privacy is also evident in Supreme Court decisions recognizing the privacy inherent in our "intimate associations with others." *See, e.g.*, Kendall Thomas, *Beyond the Privacy Principle*, 92 COLUM. L. REV. 1431, 1445-46 (1992) (quoting Bowers v. Hardwick, 478 U.S. 186, 206 (1986) (Blackmun, J., dissenting)).

[283] *See supra* note 274 and accompanying text.

There *is*, therefore, a middle ground between "private" and "public"; I can claim Fourth Amendment privacy without having to exclude *everyone* from my spaces, my activities, and my communications.[286] But this notion of "shared privacy" seems to be limited; currently, the only relationship that clearly supports a non-zero-sum conception of privacy is the intimate relationship that exists between those who reside together.[287] That is no doubt because this principle is artefactual; the Fourth Amendment and its common law antecedents were, after all, primarily concerned with protecting the "castle," the home, from unauthorized government intrusions.[288]

---

[284] *See supra* notes 281-; *see also* Coombs, *supra* note 280, at 1618 ("One reason we protect the legal right to exclude others is to empower the owner to choose to share his home or other property with his intimates"); James B. White, *The Fourth Amendment as a Way of Talking About People: A Study of Robinson and Matlock,* 1974 SUP. CT. REV. 165, 217 ("Part of the . . . personal privacy is . . . social or communal privacy, the interest people have in the security of their arrangements for sharing what they have with others.").

I do assume the risk of treachery on the part of those with whom I share my home. If, for example, my spouse decides to collect evidence of my criminal activity from our home and take it to the police, I cannot complain. My privacy may have been compromised, but not by state actors. *See, e.g.,* Coolidge v. New Hampshire, 403 U.S. 443, 487-90 (1971).

[285] O'Connor v. Ortega, 480 U.S. 709, 730 (1987) (Scalia, J., concurring).

[286] For more on this, *see infra* Section III.B.2.

[287] *See, e.g.,* Reardon v. Wroan, 811 F.2d 1025, 1027 n.2 (7th Cir. 1987) (holding that members of fraternity had a reasonable expectation of privacy in their fraternity house because a fraternity is an exclusive living arrangement with the goal of maximizing the privacy of its affairs). In *O'Connor v. Ortega,* a majority of the Supreme Court held that a physician had a reasonable expectation of privacy in his office, but only because he "did not share his desk or file cabinet with any other employees." *O'Connor*, 480 U.S. at 718-19.

[288] *See supra* Section I.A. *See, e.g.,* Oysted v. Shed, 13 Mass. 520, 522-23 (Mass. 1816):

> The authorities do not clearly show what persons are considered as belonging to the family of a householder, and so having a right to protection under his castle. The very learned judges, *Foster, Hale,* and

How, you may ask, does this narrow non-zero sum conception of privacy pertain to our inquiry into whether we can adopt the more expansive interpretation of the Fourth Amendment that is needed to address the consequences of pervasive technology?[289] It gives us a second alternative, so that we have two conceivable ways of frustrating the "harvesting" scenario:[290] one is to continue to rely on the "assumption of risk" calculus and put the onus on individuals to prevent identifiable personal data from leaking into the "public" domain,[291] and the other is to expand the non-zero sum conception of privacy outlined above so it protects the sharing of personal information in relationships other than those based on common occupancy of a home. These alternatives are examined below.

### 1. Risk

If we apply the "assumption of risk" calculus,[292] the only way we, as individuals, can frustrate the "harvesting" dynamic is to ensure that our personal information does not fall into the hands of third-parties, e.g., service providers, online merchants, etc.[293] This approach in effect continues the spatial conception of privacy: If I use barriers and other devices to shield my information from others, it is private; if I do not employ such efforts, or if they are futile, I knowingly expose my information to "public" view and it loses any claim to Fourth Amendment protection.[294]

---

> *Coke* . . . say, that the outer doors or windows shall not be forced by an officer, in the execution of civil process against the occupier or any of his family, who have their domicil or ordinary residence there . . . . According to these principles, not only the children and the domestic servants of the occupier are . . . entitled to protection; but, also, permanent boarders, or those who have made the house their home, may properly be considered as a part of the family.

*Id.* at 522-23

[289] *See supra* note 275 and accompanying text.

[290] *See supra* Section III.A.

[291] *See supra* note 274 and accompanying text; *see also* Section II, *supra*.

[292] *See supra* note 274 and accompanying text; *see also* Section II, *supra*.

[293] *See supra* Section III.A.

[294] *See supra* note 274 and accompanying text; *see also* Section II, *supra*.

The problem with this approach is that the "assumption of risk" calculus is an unreasonable methodology for a non-spatial world. It assumes, as noted earlier, that I have a choice: to reveal information by leaving it unprotected or to shield it from "public" view.[295] In the real, physical world, these options make sense: I can shield my activities from public scrutiny by drawing the curtains in my living room, installing a fence around my backyard, putting lock on my doors, etc. Inherent in the "assumption of risk" calculus is the assumption that I am *able* to withdraw information about myself (my activities, my health, my preferences) from the public domain. This assumption will continue to retain its validity for the spatially-based activities of my life: I can frustrate my nosy neighbor's attempt to ascertain what I do in the evenings by closing the curtains and employing whatever other devices real-world technology gives me to exclude the physically prying eye. But how can I do this in a world of pervasive technology, a world in which I am necessarily surrounded by devices that collect data and share it with external entities?

This is the *Smith-Miller* problem:[296] In *Smith v. Maryland,* the Supreme Court held that Smith had no "expectation of privacy" in the numbers he dialed from his home telephone.[297] The Court held that Smith "voluntarily conveyed numerical information to the telephone company and 'exposed' that information . . . . In so doing," he "assumed the risk that the company would reveal to police the numbers he dialed."[298] The problem with this holding is that it erroneously assumes Smith had a choice. In fact, since had no way to shield the numbers he dialed from the telephone company, the only choice Smith had to minimize his risk of being observed was to leave home and use a pay phone.[299]

---

[295] *See supra* Section II.B.

[296] *See supra* Section I.B.

[297] *See* Smith v. Maryland, 442 U.S. 735, 744 (1979); *see also supra* Section I.B.

[298] *Smith*, 442 U.S. at 744. *See supra* Section I.B.

[299] *See, e.g., Smith*, 442 U.S. at 749-50 (Marshall, J., dissenting):

> Implicit in the concept of assumption of risk is some notion of choice. At

That may seem a trivial matter, but consider the implications this decision has for life in a world of more pervasive technology: I install an alarm system in my home; it lets the security company monitor my routines (when I retire and arm the system, when I rise and disarm it), my comings and goings (arming and disarming the system each time) and the extent to which I give others access to my home (canceling false alarms, adding new user codes, etc.). Under *Smith*, I have no reasonable expectation of privacy in the data gathered by the security company because I voluntarily allowed the company to collect this information without encrypting or otherwise shielding it from their review; of course, if I did that (assuming I was able to do so), it would frustrate the purpose of the alarm system. My only choices under *Smith*, therefore, are to (i) trade security for privacy or (ii) trade privacy for security.[300]

The evolution and proliferation of more pervasive, more complex technologies will present us with other, equally-illogical choices. If I am elderly and choose to live in one of the "smart homes" currently being developed, have I surrendered all privacy? The home monitors my activities, my intake of food and medications, my temperature, my sleep and wake cycles, my interactions with vendors and with friends; its embedded systems interact with me and, in so doing, compile data continually.[301] The home uses this data to assess whether I need

---

> least in the third-party consensual surveillance cases, which first incorporated risk analysis into Fourth Amendment doctrine, the defendant presumably had exercised some discretion in deciding who should enjoy his confidential communications. By contrast here, unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative.

*Id.* (citing Lopez v. United States, 373 U.S. 427 (1963); Hoffa v. United States, 385 U.S. 293 (1966); United States v. White, 401 U.S. 475 (1971) (plurality opinion)).

[300] *See supra* note 299.

[301] *See, e.g.,* Cory D. Kidd, et al., *The Aware Home: A Living Laboratory for Ubiquitous Computing Research* 7, GEORGIA INSTITUTE OF TECHNOLOGY—THE AWARE HOME RESEARCH INITIATIVE (1999), *available at* http://www.cc.gatech.edu/fce/ahri/publications/cobuild99_final.PDF ("An important issue that must be addressed . . . is . . . privacy. The home is constantly monitoring the occupants'

assistance, perhaps to order food and other necessities for me and to call for assistance if I seem ill or injured. In so doing, it shares data about me with its central control center and with a host of other entities. By choosing to live in such a home, again for the sake of security, have I surrendered all privacy in the data it compiles?[302]

This question arises for any technology that results in the collection of personal data.[303] Essentially, *Smith* presents us with a Hobson's choice:[304] Embrace technology and surrender privacy in the data it compiles and disseminates or reject technology and thereby prevent the exposure of one's personal data. The problem with this equation is that one must become a Luddite to frustrate the "harvesting" dynamic.[305] It ignores the fact that we are not living in the seventeenth century; we live in an environment in which technology is an increasingly essential, invisible component of our lives.[306] There is no twenty-first century analogue of the adhesive envelope.[307] I may be able to encrypt the contents of my communications,[308] but I cannot shield my online activity from my service provider, conceal the nature and extent of my online purchases, or mask information generated by systems in my home, my office, and my vehicle. There can, therefore, be no legitimate inference that in sharing that information with that narrow circle I am willing to share it with the entire world or with the government.

*Smith* is another *Olmstead.* When *Olmstead* was decided,

---

whereabouts and activities, using audio and video observation methods, and even tracking its inhabitants' medical conditions").

[302] The same question arises, of course, if I choose to live in such a home merely because of convenience.

[303] *See supra* Section III.A.

[304] A *Hobson's choice* is a choice with no real alternative. *See Hobson's choice*, Dictionary.com, at http://dictionary.reference.com/search?r=10&q=Hobson's%20choice (last visited Aug. 16, 2005).

[305] *See supra* Section III.A.

[306] *See supra* Section II.

[307] *See supra* notes 54-55 and accompanying text.

[308] *See, e.g., About Hushmail*, Hushmail.com, at http://www.hushmail.com/about?PHPSESSID=994c85ba654ae97074f261d2dceb5190 (last visited Aug. 16, 2005).

the technology was in place but the implications were not clear; by the Supreme Court decided *Katz*, it had become clear what was at stake in wiretapping. When *Smith* was decided a quarter of a century ago, the Internet was in its infancy and personal computers had yet to appear; the technology was not yet in place, and so the implications were not clear.[309] We are now approaching a critical set of issues—the effects of technology of an unparalleled sophistication on our privacy. While the *Katz* "assumption of risk" calculus may still be valid for traditional activity in the real, physical world, it cannot be used to operationalize privacy in an era of pervasive technology.[310] The sophistication and functionality of these technologies means that the element of choice is lacking. Our only hope, therefore, for frustrating the "harvesting" scenario is to expand the non-zero-sum conception of privacy outlined above.[311]

### 2. Relationship

*Smith* is another *Olmstead* conceptually, as well as in the more pragmatic sense noted above.[312] The Supreme Court held that Roy Olmstead did not have a Fourth Amendment expectation of privacy in the content of his telephone communications because he used a "telephone instrument" with "connecting wires" to "project his voice to those quite outside" his home.[313] The *Olmstead* majority did not recognize that Olmstead was not broadcasting the content of his communications to the world at large; instead, he was making a controlled, focused disclosure of communicative content to an identified individual over a network inaccessible to one not equipped with specialized interception devices.[314]

---

[309] *See, e.g.*, Barry M. Leiner, *et al.*, *A Brief History of the Internet*, at http://www.isoc.org/internet/history/brief.shtml#Initial_Concepts (last visited Aug. 16, 2005).

[310] The Supreme Court recognized this, at least to some extent, when it held that using thermal imaging technology to detect information from inside a home is a search under the Fourth Amendment. *See* Kyllo v. United States, 533 U.S. 27, 34 (2001) (to hold otherwise would "be to permit police technology to erode the privacy guaranteed by the Fourth Amendment").

[311] *See supra* Section III.B.

[312] *See supra* Section III.B.1.

[313] *See supra* note 105.

The *Katz* Court understood this and therefore reversed *Olmstead*.[315] The *Smith* Court somehow failed to see the analogy between Katz conveying substantive data via the telephone company and Smith conveying switching information to the telephone company.[316] If we take the *Katz* Court at its word, and operate on the premise that the Fourth Amendment protects "people, not places,"[317] the result should be the same in both cases.[318] If substantive, consciously intelligible communication is protected (the conversation), nominally intelligible data should be protected as well.

To understand why that is so, we must consider the implications of the non-zero-sum conception of privacy outlined earlier.[319] That so far narrow conception of privacy recognizes a middle ground between "private as sequestered" and "public."[320] It derives from common law principles that anteceded the Fourth Amendment and were intended to secure citizens' right to enjoy the "intimate activities" of the home free from arbitrary intrusions by government authorities.[321] As noted earlier, these common law principles recognized a concept of "shared privacy" based upon certain relationships—e.g., family members, servants, guests—and this concept was implicitly incorporated into the Fourth Amendment.[322]

---

[314] *See supra* Section I.A.3.

[315] *See supra* Section I.A.3.

[316] *See supra* Section I.B.; *see also* Section I.A.3.

[317] *See supra* note 122 and accompanying text.

[318] *See, e.g.*, *Smith*, 442 U.S. at 752 (Marshall, J., dissenting):

> Just as one who enters a public telephone booth is 'entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world,' . . . so too, he should be entitled to assume that the numbers he dials in the privacy of his home will be recorded . . . solely for the phone company's business purposes. Accordingly, I would require law enforcement officials to obtain a warrant before they enlist telephone companies to secure information otherwise beyond the government's reach.

*Id.* (quoting *Katz*, 389 U.S. at 352).

[319] *See supra* Section III.B.

[320] *See supra* Section III.B.

[321] *See supra* Section I.A. *See, e.g.*, United States v. Dunn, 480 U.S. 294, 301 n.4 (1987) (Fourth Amendment intended to protect the "intimate activities associated with domestic life and the privacies of the home"); Dow Chemical Co. v. United States, 476 U.S. 227, 236 (1986) (Fourth Amendment protects the "intimate activities associated with family privacy and the home"); *see also supra* Section III.B.

Building on *Ex parte Jackson*,[323] the *Katz* Court recognized that this shared privacy was portable, i.e., could survive transmission from one private enclave (home, office, telephone booth) to another.[324] Interestingly, neither of the communications at issue in these cases involved the "intimate activities" of the home, the original locus of shared privacy: Ireland Jackson mailed a lottery circular,[325] and Charles Katz was a bookie who called a gambler to place bets for his customers.[326] Both cases recognized a Fourth Amendment expectation of privacy in the content of secure communications—including "commercial" communications—that are in transit to another. The fact that the contents were to be revealed to another person was not fatal because the sender had taken steps to ensure that the information was only communicated to that person; both Jackson and Katz, in other words, were attempting to make a controlled disclosure of information to another person.

Now, one can argue that the result in these cases is irrelevant to the point under consideration here—the privacy of information conveyed to third parties—because both of these cases were concerned with "sealed" information that *had not yet been revealed to another*. Viewed in this light, these cases can be seen as involving nothing more than an application of the "assumption of risk" principle:[327] By employing measures to secure (adhesive envelope, phone booth)[328] the contents of their communications, Jackson and Katz had a Fourth Amendment expectation of privacy in their contents until they reached their respective destinations. In this view, the contents of Jackson's circular and of Katz's calls were private only while they were in transit; once they reached the recipients they were no longer private because they had been communicated to another person.

---

[322] *See supra* Section III.B.

[323] *See supra* Section I.A.1.

[324] *See supra* §§ I(A)(1) and I(A)(3); *see also Katz*, 389 U.S. at 352 (citing *Jackson* for the proposition that what one seeks to preserve as private, even in a "public" area, can be protected by the Fourth Amendment).

[325] *See supra* Section I.A.1. Jackson was indicted for "unlawfully depositing . . . in the mail of the United States . . . a circular concerning a lottery . . . enclosed in an envelope addressed to one J. Ketcham, at Gloversville, New York." *Ex parte* Jackson, 96 U.S. 727, 727 (1877).

[326] *See, e.g.*, William W. Greenhalgh & Mark J. Yost, *In Defense of the "Per Se" Rule: Justice Stewart's Struggle to Preserve the Fourth Amendment's Warrant Clause*, 31 AM. CRIM. L. REV. 1013, 1068 (1994).

But why must it follow that a "private" communication inevitably ceases to be private once the information it contains has been received? This proposition apparently rests on the assumption that by revealing information to another I assume the risk she will prove unfaithful and reveal that information to the police. But we recognize a narrow concept of shared privacy which encompasses communications and activities we reveal to those with whom we share the "intimate activities" of the home, even though they, too, could prove unfaithful.

This concept of shared privacy is so embedded in our history and culture that the reasons for its existence are seldom articulated.[329] Clearly, though, it is based on two considerations: (1) It facilitates intimacy and security in our domestic lives, which would be poor and solitary[330] if we had to shield our every word and action from those with whom we live; and (2) it encompasses disclosures made to those with whom we share a relationship that makes it "reasonable" to assume they will respect the limited nature of these disclosures.[331] These considerations differentiate this shared domestic privacy from the line of cases in which the Supreme Court has held that wrongdoers assume the risk of the disclosures they make to our criminal associates.[332] Recognizing shared privacy among criminal confreres would serve no useful purpose and would run contrary to the pragmatic observation that there is no honor among thieves.

---

[327] *See supra* note 274 and accompanying text; *see also* Section II, *supra*.

[328] *See supra* §§ I(A)(1) and I(A)(3).

[329] *See generally supra* Section III.B.

[330] *See supra* note 285 and accompanying text. In *Leviathan*, Thomas Hobbes described the life of man in a state of nature as "solitary, poor, nasty, brutish, and short." THOMAS HOBBES, LEVIATHAN, *available at* http://oregonstate.edu/instruct/phl302/texts/hobbes/leviathan-c.html#CHAPTERXIII (last visited Aug. 15, 2005).

[331] *See generally supra* Section III.B.

We may want miscreants to betray each other, but that should not be true for other, legitimate relationships. Trust is a fundamental principle of democracy; we need to be able to trust those with whom we have certain relationships, and we need to be able to trust that law enforcement will respect those relationships.[333] Otherwise, we descend into a state of paranoia and keep each other at arm's length;[334] this is the basic flaw in the "assumption of risk" principle. In a world of evolving technology, it results in an "arm's race" in which I have a reasonable expectation of privacy only as long as and insofar as my technology successfully frustrates law enforcement efforts to subject my activities to scrutiny.[335] And there is nothing I can do to maintain informational privacy[336] as long as we insist that any disclosure of information not encompassed by the narrow conception of shared privacy outlined earlier automatically puts that information in the "public" domain.[337]

---

[332] *See, e.g.,* Hoffa v. United States, 385 U.S. 293, 302 (1966) (Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.").

[333] *See, e.g.,* Erik Luna, *Transparent Policing,* 85 IOWA L. REV. 1107, 1158-60 (2000):

> Trust is . . . a fundamental ingredient of modern liberal democracy, with social contract theorists maintaining that consent grounded in public trust provides the very basis for governmental authority . . . . Distrust leads to the self-interested atomization of the citizenry and a lack of cooperation within the community. Most importantly, popular mistrust of government undermines the perceived legitimacy of the law, which in turn reduces public compliance with legal commands.

*Id.* (notes omitted).

[334] *See supra* note 333.

[335] *See supra* Section III.B.1. *See, e.g.,* Scott Granneman, *Email Privacy Is Lost,* SECURITY FOCUS (July 29, 2004), at http://www.securityfocus.com/columnists/258 ("This is an arms race. Every time the technology changes to enable further surveillance, something happens to render that surveillance inoperable . . . at least until the next technological change.").

[336] *See supra* note 159 and accompanying text.

Can we alter the latter principle? Would it be "reasonable" to incorporate another, broader conception of shared privacy into the Fourth Amendment in order to protect the privacy of information I share with certain third parties? Would such a step be fundamentally inconsistent with the history and purposes of the Fourth Amendment?

We could extrapolate such a principle from the narrower conception of shared privacy that anteceded and was implicitly incorporated into the Fourth Amendment. The critical issue is deciding how far we want to go in protecting information held by various third parties.

Let us begin with the easiest case. The current conception of shared privacy evolved to protect the "intimate activities" of the home and, as such, encompassed those who were privy to such activities, e.g., family, houseguests, and servants.[338] We cannot "reasonably" construe third-party information holders as family members or houseguests because the familial and residential ties are lacking; even entities that provide alarm and other services and that will interact with systems in "smart homes" do so remotely, from some other physical location. But these entities are functionally analogous to "servants" who are also encompassed by this conception of shared privacy; unlike the servants of centuries ago, they do not reside in the home, but they provide services that promote and sustain activities within the home. And we maintain a relationship with them that is analogous to the relationship householders of the common law era maintained with their servants; the basis of this relationship is a pecuniary arrangement, but it also involves continuity and trust.

We rely on "servant" entities for support; we may sometimes switch between entities, but this is the exception; our preferred mode is one of stability in which we have established, ongoing relationships with entities that provide the various types of support we require. It is reasonable to anticipate that the continuity of these relationships will increase as we come to rely on increasingly complex, interdependent technologies; it is one thing to change our telephone company, quite another to modify a multi-functional network.[339] The other notable feature of these relationships is trust:[340] We give those with whom we have established such a relationship access to personal, "private" information so they can discharge the functions for which they are employed.[341] We do, as the *Smith* Court said,

---

[337] *See supra* Section I.B.

[338] *See supra* Section III.B.

---

[339] *See supra* Section II.

[340] *See, e.g.,* State v. Hunt, 91 N.J. 338, 346-47, 450 A.2d 952, 956 (1982):

> The telephone caller is . . . entitled to assume that the numbers he dials in the privacy of his home will be recorded solely for the telephone company's business purposes. From the viewpoint of the customer, all the information which he furnishes with respect to a particular call is private. The numbers dialed are private. The call is made from a person's home or office, locations entitled to protection under . . . Article I, par. 7 of the New Jersey Constitution.

*Id.*

[341] *See supra* Section II.

Some states have recognized a reasonable expectation of privacy in third-party records under their own constitutions. *See, e.g.,* State v. McAllister, 366 N.J. Super. 251, 264-65, 840 A.2d 967, 975-76 (2004):

> [W]e hold that there exists a reasonable expectation of privacy in a person's bank records. . . . We are in full accord with Justice Mosk's articulation of the pervasiveness of the need to make and maintain bank records as an incident of private, personal financial life and participation . . . in modern economic life. . . .
>
> The discomfort in finding a stranger poring over one's checkbook, deposit slips and cancelled checks is equal to seeing someone . . . reviewing a list of dialed telephone numbers called from home . . . . Banks, like telephones, are an extension of one's desk or home office. Indeed, as in the case of the telephone, technological advances in the form of personal computers with access to the internet and electronic banking services have made those services available to the homes of its depositors. Bank records kept at home could not be seized in the absence of a duly issued search warrant based upon probable cause and they should not be vulnerable to viewing, copying, seizure or retrieval simply because they are readily available at a bank.
>
> Finally, the fact that financial affairs are memorialized in written records of banks or maintained in their electronic data systems to which, as part of its legitimate business, a bank's employees have access, does not suggest that persons have any sense that their private and personal traits and affairs are less confidential when they deal with their bank than when they make telephone calls . . . . The repose of confidence in a

voluntarily convey information to these entities,[342] but we do not do so recklessly, or promiscuously; we convey information to our "servant" entities in a secure fashion intending that it be used only for the purpose of allowing the entity to perform the services for which we have contracted.[343]

---

> bank goes beyond entrustment of money, but extends to the expectation that financial affairs are confidential except as may be reasonable and necessary to conduct customary bank business.

*Id.* (citing Burrows v. Superior Court, 13 Cal. 3d 238, 118 Cal. Rptr. 166, 172, 529 P.2d 590 (1974)). States have also rejected the logic of *Smith. See, e.g.,* People v. Spoerleder, 666 P.2d 135, 141 (1983):

> A telephone is a necessary component of modern life. It is a personal and business necessity indispensable to one's ability to effectively communicate in today's complex society. When a telephone call is made, it is as if two people are having a conversation in the privacy of the home or office . . . . The concomitant disclosure to the telephone company, for internal business purposes, of the numbers dialed by the telephone subscriber does not alter the caller's expectation of privacy and transpose it into an assumed risk of disclosure to the government. . . .
>
> We view the disclosure to the telephone company of the number dialed as simply the unavoidable consequence of the subscriber's use of the telephone as a means of communication . . . . Any use the telephone company might make of such information for its own internal accounting purposes is far different from governmental evidence gathering. . . .
>
> . . . .
>
> One's disclosure of certain facts to the telephone company as a necessary concomitant for using an instrument of private communication hardly supports the assumption that the company will voluntarily convey that information to others. Telephone companies are in the business of providing telephone subscribers with the equipment necessary for electronic communication in today's world. . . . The expectation that information acquired by the telephone company will not be transferred . . . to the government for use against the telephone subscriber appears to us to be an eminently reasonable one.

*Id.*; *see also* State v. Thompson, 114 Idaho 746, 750-51, 760 P.2d 1162, 1166-67 (1988) (use of a pen register is a search requiring a warrant under Idaho Constitution).

[342] *See supra* Section I.B.

[343] *See Smith*, 442 U.S. at 749 (Marshall, J., dissenting): "Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes." *See, e.g.,* State v. Mollica, 114 N.J. 329, 344-45, 554 A.2d 1315, 1323 (1989) (police must obtain search warrant to secure telephone records); *see also supra* note 338.

We trust our "servant" entities not to reveal our personal information to tabloids, disgruntled relatives, and other "civilians," and they generally live up to our expectations. Why, then, is this relationship, and the information it generates, not within the Fourth Amendment?[344] The obvious response to this question is that bringing this relationship within the Fourth Amendment is unnecessary since these entities are not *obligated* to provide this information to law enforcement. This, however, ignores reality.[345] A private entity may find it unsettling to refuse to cooperate with law enforcement, or may not understand the consequences of doing so, in terms of larger-scale privacy issues.[346] And a subpoena can be used to compel a truly reluctant entity to provide this information without providing the protection accorded under a warrant.[347]

The critical question is who should bear the risk: the individual (who currently loses privacy by sharing information with external entities) or law enforcement (which will have to demonstrate individualized suspicion to obtain shared information if we define it as private).[348] If we bring this information

---

[344] One might argue that the information itself is not worthy of protection because while it is data that can give rise to inferences about activities taking place within the home, this information does not, in and of itself, describe such activities. The Supreme Court rejected a similar argument in *Kyllo v. United States*, 533 U.S. 27, 37 ("The Fourth Amendment's protection of the home has never been tied to . . . the quality . . . of information obtained"); *see also supra* Section I.A.4.

[345] *See supra* note 266.

[346] *See supra* note 248.

[347] *See, e.g.,* United States v. Miller, 425 U.S. 435, 437 (1976).

[348] *See* PERSONAL PRIVACY IN AN INFORMATION SOCIETY: THE REPORT OF THE PRIVACY PROTECTION STUDY COMMISSION, CHAPTER 9 (1977), http://aspe.hhs.gov/datacncl/1977privacy/c9.htm:

> The balance to be struck is an old one; it reflects the tension between individual liberty and social order. The sovereign needs information to maintain order; the individual needs to be able to protect his independence and autonomy should the sovereign overreach. The peculiarly American notions of legally limited government and the protections in the Bill of Rights provide broad . . . standards for reaching a workable balance. But the world has a way of disrupting the particular balance struck in past generations; the theory may remain unaltered but circumstances change, requiring a reworking of the mechanisms which maintained the

within the Fourth Amendment by incorporating a shared privacy principle into our Fourth Amendment doctrine, we (1) enhance the security of the relationship between individuals and their "servant" entities, thereby enhancing privacy and trust; and (2) do not put this information totally outside the reach of law enforcement. Bringing this information within the Fourth Amendment simply means that to obtain information from "servant" entities, law enforcement officers have to obtain a warrant supported by probable cause.[349] That reduces the possibility that the officers will be able to bypass the protections of the Fourth Amendment by utilizing the "harvesting" scenarios outlined earlier[350] and ensures that we maintain the proper balance between privacy and law enforcement.[351]If we incorporate this conception of shared privacy into our Fourth Amendment doctrine, we will then have to address a secondary issue: Do we limit shared privacy to information generated by relationships directed at our homes, or do we expand it out to encompass any relationship with a "servant" entity? Do we, in other words, recognize shared privacy in the information individuals engaging in commercial, professional and service endeavors share with their "servant" entities, as well? If we do that do we also extend the concept to encompass the relationship commercial, educational and other entities share with their "servant" entities? Or do we limit shared privacy to information that can, in effect, be used to gain access to the activities within our homes?

Those are difficult questions, the resolution of which is quite beyond the scope of this essay. Essentially, they raise two dichotomies: individual and entity; home and not-home. Extending Fourth Amendment principles to encompass informa-

---

balance in the past.

*Id.*

[349] *See supra* note 341.

[350] *See supra* Section III.A.

[351] It has the added advantage of eliminating the current, increasingly unworkable, distinction between content information and "other" information. *See, e.g.*, Susan Freiwald, *Uncertain Privacy: Communication Attributes After The Digital Telephony Act*, 69 S. CAL. L. REV. 949, 954-58 (1996).

tion an individual shares with a "servant" entity that provides support services for the individual's home is the easiest scenario because it is the closest to the spatially-based conception of privacy upon which the Fourth Amendment is predicated.[352] Extending Fourth Amendment shared privacy to encompass the information an individual shares with a "servant" entity that provides support services to the individual's place of business seems to be more of a stretch, simply because we think of places of business as inherently "public." But the Supreme Court has extended traditional Fourth Amendment spatial privacy to places of business;[353] officers therefore must get a search warrant to seek evidence they believe is located in commercial or professional offices.[354] We could, therefore, "reasonably" extend shared privacy to individually-owned places of business; our primary concern, after all, is with protecting the privacy of individuals,[355] and information-sharing in this context involves a relationship initiated by an individual. Such an extension of shared privacy would also recognize the extent to which we conduct "personal" matters that were once limited to our homes, from our offices.[356]

---

[352] *See supra* Section I.A.

[353] *See* Marshall v. Barlow's, Inc., 436 U.S. 307, 311-12 (1978):

> The . . . Fourth Amendment protects commercial buildings as well as private homes. To hold otherwise would belie the origin of that Amendment, and the American colonial experience. . . . The general warrant was a recurring point of contention in the Colonies immediately preceding the Revolution. The particular offensiveness it engendered was acutely felt by the merchants and businessmen whose premises and products were inspected for compliance with the several parliamentary revenue measures that most irritated the colonists. '[The] Fourth Amendment's commands grew in large measure out of the colonists' experience with the writs of assistance . . . [that] granted sweeping power to customs officials and other agents of the King to search at large for smuggled goods.' Against this background, it is untenable that the ban on warrantless searches was not intended to shield places of business as well as of residence.

*Id.* (citations omitted) (quoting United States v. Chadwick, 433 U.S. 1, 7-8 (1977)).

[354] *See* Camara v. Municipal Court, 387 U.S. 523, 528-529 (1967); See v. City of Seattle, 387 U.S. 541, 543 (1967).

[355] *See supra* note 353 (privacy of "merchants and businessmen").

[356] It would also eliminate conceptual difficulties that would arise when someone's home and office were physically located on the same premises.

The entity/not-home option is more problematic. The Supreme Court has held that "corporations can claim no equality with individuals in the enjoyment of a right to privacy."[357] Since privacy is a personal construct, it seems we cannot justify extending shared privacy to artificial entities, unless we were to decide such a step is necessary to protect the privacy of individuals associated with the artificial entity. Of course, if we felt that such a step was necessary, the more logical approach would be to focus on the individuals, not the artificial entity; that is, we could decide to extend the concept of shared privacy to encompass an individual's relationship with an artificial entity that was not engaged in providing support services to the individual's home or office. This would protect the individual's information-sharing with the artificial entity without requiring us to extrapolate an individually-based notion of shared privacy (e.g., individual-individual and individual-"servant" entity) to a collective entity.

## IV. CONCLUSION

Ubiquitous technology presents us with the challenge of deciding how we want to apply the Fourth Amendment in a world that is very different from the world from which it sprang.[358] Informational privacy[359] was almost nonexistent in the seventeenth and eighteenth centuries; in that world there were no computers, no copying machines, no credit card transactions, no telephones or other services provided by externalities, no insurance companies, no educational or employment records, none of the kinds of data we routinely generate in the course of our lives.

Citizens of that era engaged in transactions with vendors, but the transactions were in cash and generated few, if any, written records;[360] while a vendor may have recalled some details of my transactions, those details were not documented and preserved in some more or less permanent form. And whatever information resulted from these transactions was in limited form; I traveled to the vendors and dealt with them externally in a "public" place. They were not privy to the details of life in my home; those details were available only to the intimates—family, guests, servants—with whom I shared the physical privacy of my home. The only records that were likely to exist as to me and my activities were in my possession: "papers" I created myself and letters from others. Since copying machines, carbon paper and other implements of replication did not exist, a "paper" was usually an original,[361] which made it relatively easy to control access to the information it contained; it could be held by only one person at a time. I could therefore physically secure my "papers" inside my home, in a chest or a cabinet, or a desk; once the common law antecedents of the Fourth Amendment appeared, it was clear that law enforcement could not enter my home to violate my privacy and inspect my "papers" without securing a warrant.[362] This was sufficient to protect my spatial and informational privacy from arbitrary governmental action; aside from physical entry into my premises, there was no other way law enforcement could access my personal information (other than the generalized, reputational information I disseminated by acting in "public" places).

---

[357] United States v. Morton Salt Co., 338 U.S. 632, 652 (1950).

[358] *See supra* Section I.A.

[359] *See supra* note 159 and accompanying text.

[360] Credit existed in the seventeenth and eighteen centuries, but it was limited to the mercantile and privileged classes. *See, e.g.*, MAUREEN WALLER, 1700:

This approach is no longer sufficient. The physical and informational barriers we once used to differentiate between our "private" and "public" selves are being eroded by technology, and the erosion is accelerating. If we persist in utilizing a zero-sum, spatial conception of privacy to implement the Fourth Amendment, we will render it ineffective as a guarantor of privacy in the face of arbitrary government action.[363] If we

---

SCENES FROM LONDON LIFE 7, 204, 242 (2000).

[361] *See, e.g.,* WALTER M. BESANT, LONDON IN THE TIME OF THE STUARTS 53 (1903) (describing seizure of the "papers" of James Howell, who was a suspected spy).

[362] *See supra* Section I.A.

[363] *See supra* Section III.A.

continue along this path, the Fourth Amendment will become, in effect, an artifact—a device that protects against a limited class of real-world intrusions (which will become increasingly unnecessary given the other alternatives).[364]

---

[364] *See supra* Section III.A.

# SEARCH WARRANTS IN AN ERA OF DIGITAL EVIDENCE

*Orin S. Kerr*[*]

## ABSTRACT

*This Article contends that the legal rules regulating the search warrant process must be revised in light of the demands of digital evidence collection. Existing rules are premised on the one-step process of traditional searches and seizures: the police obtain a warrant to enter the place to be searched and retrieve the property named in the warrant. Computer technologies tend to bifurcate the process into two steps: the police first execute a physical search to seize computer hardware, and then later execute a second electronic search to obtain the data from the seized computer storage device. The failure of the law to account for the two-stage process of computer searches and seizures has caused a great deal of doctrinal confusion, making it difficult for the law to regulate the warrant process effectively. The Article concludes by offering a series of proposed amendments to Rule 41 of the Federal Rules of Criminal Procedure to update the warrant process for the era of digital evidence.*

## INTRODUCTION

Search warrants provide one of the basic tools for collecting evidence in criminal investigations. The history and text of the Fourth Amendment focus heavily on regulating their use.[1]

---

[*] Associate Professor, George Washington University Law School. This paper was commissioned and underwritten by funds from the National Center for Justice and the Rule of Law at the University of Mississippi School of Law (National Center), which is supported by a grant from the Office of Justice Programs at the United States Department of Justice (2000-DD-VX-0032). Thanks to Tom Clancy, Susan Brenner, and Christopher Slobogin for comments on an earlier draft.

[1] *See* U.S. CONST. amend. IV ("The right of the people to be secure in their

In recent decades, the traditional Fourth Amendment standards governing the warrant process have been supplemented with comprehensive statutory rules such as Rule 41 of the Federal Rules of Criminal Procedure.[2] Today, the combination of statutory and constitutional rules creates a well-defined procedure for obtaining and executing search warrants familiar to every police officer, detective, and prosecutor.

This article argues that the warrant process must be reformed in light of the new dynamics of computer searches and seizures. In the last two decades, the widespread use of computers has led to a new kind of evidence in criminal cases: digital evidence, consisting of zeros and ones of electricity. In a recent essay, I argued that the rise of digital evidence will trigger the need for a "new criminal procedure"—a new set of procedural rules to regulate the acquisition of digital evidence in criminal investigations.[3] This article applies that framework to the warrant process. It explains how the new facts of computer searches and seizures require changes in the laws governing the warrant process to update that law for the era of digital evidence.

The basic theory is a simple one. The existing law governing the warrant process presumes single-step searches common to the collection of traditional physical evidence. In these cases, the investigators enter the place to be searched, seize the property named in the warrant, and leave. With computer searches, however, the one-step search process is replaced by a two-step search process. The investigators enter the place to

---

persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."). For a history of the Fourth Amendment and its focus on regulating the warrant process, see NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION (1937).

[2] FED. R. CRIM. P. 41. Each state has equivalent state statutory warrant provisions. *See, e.g.,* CAL. PENAL CODE §§ 1523-42; DEL. CODE ANN. tit. 11, §§ 2304-10 (2005).

[3] Orin S. Kerr, *Digital Evidence and the New Criminal Procedure,* 105 COLUM. L. REV. 279, 308 (2005).

be searched; seize the computer hardware; take the hardware off-site; and then later search the equipment for data that may be evidence of crime.[4] Two searches occur instead of one. The physical search comes first and the electronic search comes second. Further, in most cases the two searches are quite distinct. They occur at different times, in different places, and are usually performed by different people.

The division of the traditional one-step warrant process into two distinct steps sets up four doctrinal puzzles for the law regulating the warrant process. First, what should the warrant describe as the property to be seized: the physical hardware seized during the first physical search, or the digital evidence obtained during the electronic search? Second, what should the warrant describe as the place to be searched: the location of the hardware, the hardware itself or the location where the electronic search will occur? Third, when must the electronic search occur: Is the timing governed by the same rules that govern the physical warrant execution, by some other rules, or by no rules at all? Finally, what record-keeping requirements apply to the electronic search and when must seized computer equipment be returned? All of these questions follow from an attempt to fit the one-step framework of existing law into the two-step framework of the new facts of computer searches and seizures.

---

[4] *See, e.g., In re* Search of 3817 W. West End, 321 F. Supp. 2d 953, 958 (N.D. Ill. 2004) [hereinafter *West End*] ("[I]t is frequently the case with computers that the normal sequence of 'search' and then selective 'seizure' is turned on its head. Because of the difficulties of conducting an on-site search of computers, the government frequently seeks (and, as here, obtains), authority to seize computers without any prior review of their contents."). As Susan Brenner and Barbara Frederiksen have written,

> In conventional searches and seizures, the execution of a warrant typically involves two stages: a "search" for evidence that is followed by the "seizure" of evidence once it has been found. . . .
>
> In off-site computer searches, the execution of a warrant involves four stages, not two: a *search* designed to locate computer equipment; the *seizure* of that equipment and its removal to another location; a thorough *search* of the contents of the equipment which is conducted at that location; and a *seizure* of relevant evidence located in the course of that search.

Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches And Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39, 82 (2002).

This article urges legislatures and rules committees to update the statutory rules that govern the warrant process in response to the new challenge of digital evidence searches. It contends that warrant rules should be amended to recognize the two-step nature of computer searches and seizures and to regulate both steps adequately and directly. Existing law requires courts to try to squeeze the two-step digital warrant process into a one-step legal framework. The courts have struggled to answer the four doctrinal puzzles and often have failed to reach coherent or satisfactory answers. Statutory rule reform is needed to resolve these difficulties and directly address the considerable policy questions they raise.

Two proposed changes are the most important. First, the law should require warrants seeking digital evidence to state the items to be searched for at *both* the physical *and* the electronic search stages. That is, the warrant should state the physical evidence that the police plan to seize at the physical stage and the electronic evidence that the forensics analysts plan to search for at the electronic stage. Second, warrant rules should be amended to require that the electronic search step proceeds in a timely fashion. Specifically, the law should require investigators to "image" seized computers and return the equipment in a reasonable period of time (such as thirty days) when the hardware is merely a storage device for evidence. When the hardware is believed to be contraband or a fruit or instrumentality of crime, investigators should be required to begin the forensic process within a specific period of time (such as sixty days) to establish whether that belief is correct. If it is not, the hardware should be returned; if it is, investigators should be permitted to retain it.

I will develop my argument in four parts. Part I explores the factual differences between how investigators typically execute a search warrant for digital evidence and how investigators typically execute a warrant for physical evidence. In a traditional case, the police enter the place to be searched, and then locate and retrieve the items found in the warrant. Computer searches follow a different model. Because the retrieval of digital evidence requires technical expertise and considerable time, the execution of a warrant for digital evidence generally involves two steps. The first is location and retrieval of the physical storage device that investigators believe contains the digital evidence, and the second is subsequent analysis of the storage device to locate the digital evidence. Instead of search and seizure, the process is more like physical search and seizure followed by electronic search and seizure.

Part II explores the four doctrinal puzzles created by the bifurcation of the one-step warrant process into two distinct steps. Should the property to be seized be the physical evidence seized at step one, or the electronic evidence searched for at step two? What is the place to be searched: the location of the physical storage device, the storage device itself or the location of the electronic search? When must the search be executed? In particular, what timing rules govern the computer forensic analysis required to execute the electronic search? Finally, what record-keeping requirements apply to the electronic search, and when (if ever) must seized computer hardware be returned?

Part III explores how courts have attempted to resolve these puzzles using existing statutory and constitutional rules. It focuses on the two primary questions that courts have considered in detail: the proper description of the property to be seized, and the timing of the computer forensic process. Courts have struggled in both areas to fit the old law to the new facts. They have approved both physical and virtual descriptions of the property to be seized, but only by letting the practical considerations of the two-step search override what would otherwise be significant defects in computer warrants. They have also failed to settle whether existing statutory law permits judges to condition warrants on the timing of the forensic process.

Part IV offers a series of specific amendments to the legal framework regulating the warrant process. It explains why the primary changes needed are statutory, not constitutional. The solution to the problem lies in amending of the statutory rules regulating the warrant process, not in altering Fourth Amendment standards. It also offers specific changes to Rule 41 and their state equivalents, including changes in how computer warrants are written and explicit regulation of the timing of the electronic search process when undertaken pursuant to a warrant.

## I. Digital Versus Physical Warrant Processes

The premise of my argument is that the facts common in digital evidence searches are different from the facts common in traditional physical evidence searches. Changes in the facts demand changes in the legal rules. This section introduces those differences, focusing on the replacement of the search-and-retrieve mechanism of traditional searches with a two-stage process that adds an electronic search to the traditional physical search and seizure. In physical searches, the investigators seek permission to look through a particular physical space for a particular piece of evidence, and then to take that evidence away. Executing a warrant for digital evidence generally adds a step. The investigator seeks permission to search a physical space for computer storage devices, and then takes away the computer storage devices that are found for analysis off-site at a later date. Weeks or even months later, the computer forensic analyst performs what is, in a sense, a second search: an electronic search for digital evidence, occurring long after the physical search for physical evidence. The dynamic is physical search, physical seizure, and then electronic search.

The following hypothetical cases explains the dynamic. The first presents a traditional investigation for physical evidence; the second presents a typical investigation for digital evidence. The contrast helps reveal how the basic process of executing a warrant for physical evidence is different in a number of ways from the process of executing a warrant for digital evidence.

### A. *Physical Searches and Physical Search Warrants*

Fred Felony is low on cash, so he decides to burglarize the home of Mr. and Mrs. Smith at 123 Main Street. One night when the Smiths are away, Fred picks the lock to the front door using locksmith tools and starts looking around for valuable property. Fred finds and takes three valuable items: an expensive stereo system, a collection of Victorian gold jewelry, and a mink fur coat. Fred takes these items back to his apartment and hides them in his bedroom closet. Then he puts his locksmith tools in a storage area underneath his kitchen sink. Fred's plan is to wait a few weeks until no one is looking for the stolen items and then to try to sell them at a local pawn shop.

The next day, the Smiths come back into town and realize that their home has been burglarized. They call the police. Imagine you are the police detective called to investigate the burglary at 123 Main Street. You arrive at the scene and quickly surmise that the front door was opened using locksmith tools. You speak to the Smiths, who report that three items have been stolen: a collection of gold jewelry, Mrs. Smith's mink coat and an expensive stereo system. You obtain detailed descriptions of these missing items, including the serial numbers of the stolen equipment and photographs of the stolen jewelry, and you then return to the police station.

Now imagine that you have good reason to believe that Fred Felony was behind the burglary, and that you also know that Fred Felony's last known address is 13 Prospect Avenue, Apartment B. You decide to apply for a search warrant to search Fred's apartment for the stolen goods. If you can find the stolen goods and the locksmith tools in Fred's apartment, you will have very strong evidence of Fred's guilt that can be used in court. You therefore apply for a warrant to search 13 Prospect Avenue, Apartment B for four items: locksmith tools, the mink fur coat, a stereo with the serial numbers of the stolen equipment, and Victorian gold jewelry matching the description that the Smiths gave you. In the affidavit to the warrant, you explain to the judge why you have probable cause to believe that evidence of the burglary will be located inside the apartment.

The judge finds probable cause and signs the warrant authorizing the search. The next morning, several officers join you in executing the search. You knock on Fred's door at 10:00 a.m. and announce, "This is the police! We have a warrant—open up!" Fred is not home, so after a brief wait the door is forcibly opened. After ensuring that the apartment is empty, you begin to search the home for the evidence in the warrant. After about ten minutes, one officer finds a set of locksmith tools in the storage area under the kitchen sink. The tools are "bagged and tagged," placed in an evidence bag and labeled appropriately. Twenty minutes later, you are looking through the bedroom and open the closet door. You immediately spot the fur coat and stereo equipment. You pick up the equipment and find the serial number to confirm the matching number on the warrant. You then look through the rest of the closet and find the collection of gold jewelry described in the warrant. You bag and tag the jewelry, coat and stereo equipment. With all of the evidence found, you leave a copy of the warrant on the front door so that Fred will know what happened when he returns home. The next day, you file a return with the judge who issued the warrant reporting everything seized from the apartment: the locksmith's tools, fur coat, jewelry, and stereo equipment.

### *B. Digital Searches and Digital Search Warrants*

Now imagine a cyber version of the same crime. This time, Fred decides to commit his crime via his computer. Instead of breaking into the Smiths' home, he decides to hack into their home computer remotely to steal credit cards and other valuable financial information. Fred logs on to the Internet from his computer at home, hacks into the Smiths' home computer, and then locates and retrieves the Smiths' credit card numbers. Fred copies the files from the Smiths' computer, and later uses the Smiths' credit card number to purchase an expensive stereo, a mink coat and some gold jewelry. When the Smiths get their credit card bill weeks later, they see the extra charges and call the police. Once again, you are the investigator called to investigate the crime. Assume that you have reason to believe that Fred Felony is behind the scheme, and you suspect he hacked into the Smiths' computer to obtain the credit card information. Once again, you want to recover the fruits of the crime: the stereo, jewelry, and mink coat.

But this time you also want something else. You want to recover the digital evidence that can prove Fred hacked into the Smiths' computer. If Fred did hack into the Smiths' computer, the computer Fred used should have clues of the crime. Granted, you cannot be sure of exactly what evidence the computer will contain. Perhaps you will find hacker tools establishing Fred's ability to commit the crime. Perhaps you will find the file containing the credit card numbers that Fred copied from the Smiths' computers. Or perhaps you will find a word processing file in which Fred wrote down the steps he took to hack into the Smiths' computer. At this point you cannot know. At the same time, there is a good chance that Fred's computer contains evidence of his hacking crime. The only way to find out is to look for Fred's computer and analyze it for evidence.

Once again, you apply for a warrant to search 13 Prospect Avenue, Apartment B. Once again you want to seize a fur coat, gold jewelry, and expensive stereo equipment. This time, however, you also request permission to take Fred's computer. You knock on Fred's door, enter the apartment, and quickly find the stereo equipment, fur coat, and jewelry. This time you also look for Fred's computer. To your surprise, however, you end up finding not one but several computers and storage devices. You find one laptop computer in the living room, a desktop computer in the bedroom, and a box of floppy diskettes and thumb drives next to the desktop computer. The number of computers and storage devices give you pause. You don't know which computer is Fred's, or which computers or diskettes (if any) may contain the evidence you are looking for. Given that you can't tell what is on the computers and storage devices without turning them on and looking through them, you decide out of an abundance of caution to call headquarters and ask to speak with a computer expert.

The computer expert tells you that, as a practical matter, you have no choice but to take all of the computers and storage devices with you and send them to a government lab for analysis. He explains that you should not turn the computers on: turning them on will alter the evidence they contain.[5] To avoid altering the evidence on the computers, he explains, a computer forensic analyst must copy each storage device using special forensic tools and conduct a sophisticated and generally time-consuming forensic analysis.[6] The computer expert also emphasizes that it can take many hours, or even days, to locate specific evidence on a computer hard drive. It is technically possible to send an expert to 13 Prospect Avenue and have him try to search the computers on-site, he explains, but it is likely to be quite time consuming. Outside of the controlled environment of a government forensic lab, he cannot guarantee that the evidence will be located properly. This won't do, you realize. You need to find the evidence, and you can't spend the next few days sitting in Fred's apartment with a technical expert looking through Fred's computers. The most practical option seems to be to "bag and tag" all of the computers and hard drives and let the technical experts figure it out later. You do that, and the next day you file a return on the warrant with the judge listing the evidence you seized: first, the stereo equipment, fur coat and jewelry; and second the laptop computer, desktop computer, and the box of floppy diskettes and thumb drives.

While the search of Fred's apartment is now complete, you are not done. You now need to send the computers and disk drives to the local government forensic lab for analysis. You ship the equipment to the lab, and wait for a response. After you don't hear back for a few weeks, you call the laboratory and ask if they have looked at your computers yet. The lab technician explains that the forensic process is very time consuming and that there is a three-month waiting list before a computer brought to the lab will be analyzed.[7]

---

[5] *See, e.g.*, U.S. DEPT. OF JUSTICE, FORENSIC EXAMINATION OF DIGITAL EVIDENCE: A GUIDE FOR LAW ENFORCEMENT 24 (2004), *available at* http://www.ncjrs.gov/pdffiles1/nij/199408.pdf.

[6] *See* BILL NELSON, ET. AL, GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS (Thomson 2004).

Several months later, you receive a call that the analysis has been completed. A computer forensic analyst performed an analysis of the various hard drives and storage devices, which required him to generate copies of each of the computer drives and perform various computer commands on the copies to try and locate the evidence they contained.[8] The technician's report informs you that the analyst found evidence of a hacking incident on one of the computers. The evidence includes hacker tools that could have been used to hack into the Smiths' computer, as well as a copy of the stolen file that contained the credit card numbers taken from the Smiths' computer. The other computer and the additional storage devices did not contain any evidence of criminal activity.

## II. FOUR PUZZLES: DIGITAL EVIDENCE AND THE INADEQUACY OF EXISTING LEGAL RULES

With the basic differences between physical evidence and digital evidence searches in mind, let's next consider how existing law regulates the two types of searches. This section illustrates how the law regulating the warrant process is attuned to the basic mechanisms of physical searches. Existing rules were designed to regulate the collection of physical evidence, and are naturally tailored to the search-and-retrieve dynamic. Application of the same rules to digital evidence cases reveals that the law no longer fits the facts. A series of doctrinal puzzles emerges, requiring investigators and judges to adjust the rules as best they can to come up with alternatives. This section explores the clash between the traditional rules and the new facts by exploring those existing rules and seeing how they apply to digital evidence warrants.

---

[7] Such delays are typical, although the actual delay may vary tremendously from case to case.

[8] I explain the computer forensics process in detail in Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. (forthcoming Dec. 2005).

At the outset, it is important to understand the basic rules of the warrant process. The basic constitutional principle shaping the warrant process is that investigators must execute narrow warrants limited by the scope of probable cause.[9] Investigators can obtain a search warrant only if they have probable cause to believe that evidence, fruits of crime, contraband or instrumentalities of crime are located in a particular physical place.[10] The warrant must name the particular property that the police have probable cause to believe will be located in the particular place to be searched.[11] Investigators can then obtain a warrant authorizing them to go to the particular place named and search for and seize that particular property.

These constitutional rules are supplemented by statutory rules, such as Federal Rule of Criminal Procedure 41.[12] Rule 41 specifies what judges can issue warrants; what form the warrants must take; what time of day warrants must be executed; how long the police have to execute the warrant; and for what kind of property warrants can be issued. Rule 41 is often quite specific. For example, Rule 41(d) contains relatively detailed rules that govern making an inventory of the property taken and informing the suspect and the court of what was taken:

> The officer taking property under the warrant shall give to the person from whom or from whose premises the property was taken a copy of the warrant and a receipt for the proper-

---

[9] *See* Maryland v. Garrison, 480 U.S. 79, 84 (1987). *Garrison* explains:

> By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit. Thus, the scope of a lawful search is [] defined by the object of the search. . . .

*Id.* (footnote omitted).

[10] *Id.*

[11] *Id.* at 84-85.

[12] FED. R. CRIM. P. 41 (reprinted in Appendix).

> ty taken or shall leave the copy and receipt at the place from which the property was taken. The return shall be made promptly and shall be accompanied by a written inventory of any property taken. The inventory shall be made in the presence of the applicant for the warrant and the person from whose possession or premises the property was taken, if they are present, or in the presence of at least one credible person other than the applicant for the warrant or the person from whose possession or premises the property was taken, and shall be verified by the officer. The federal magistrate judge shall upon request deliver a copy of the inventory to the person from whom or from whose premises the property was taken and to the applicant for the warrant.[13]

Rule 41 also provides a mechanism by which a suspect can move for the return of property unlawfully seized.[14] The police have a right to retain the property permanently, however, if it is contraband, a fruit or instrumentality of crime. If the property is mere evidence, they generally can retain it so long as there is a plausible claim of law enforcement need.

These constitutional and statutory rules work quite naturally in the case of physical evidence. This is true for two basic reasons. First, the rules fit the facts of searches for physical evidence. Physical searches generally follow a search-and-retrieve dynamic. Physical evidence generally can be identified and retrieved from a physical place in a matter of minutes or hours. The warrant authorizes the police to enter the physical property, locate, and then retrieve the evidence named in the warrant.[15] In Fred Felony's first hypothetical, for example, the police could enter Fred's apartment and look for the mink coat, stereo equipment, jewelry and locksmith tools. Once they found those items, the investigators could take them away but had to stop searching.

The second reason these rules work with physical evidence searches is that they ensure that the police obtain physical property in a relatively narrow way that minimizes the intrusion onto the suspect's property and privacy. Each of the basic rules attempts to limit and channel police conduct based on the facts of how physical searches for physical evidence work. The particularity requirement limits *where* the police can search. They can only search the physical premises named in the warrant, such as Fred's apartment. The probable cause requirement and statutory rules on executing warrants limit *when* the search can occur; excessive delay may lead the warrant to become stale, and statutory rules govern the time windows in which the search can occur. The particularity requirement of what property is to be seized governs *how* the search occurs; general rummaging through the target's property is not permitted. Finally, a number of the statutory rules add record-keeping requirements designed to facilitate oversight and judicial review, such as the requirement that an inventory of the property be taken, the filing of a return with the court, and the allowance for motions to return physical property.

---

[13] *Id.* 41(d).

[14] *Id.* 41(g).

[15] *See* Appendix.

A very different picture emerges when we try to apply the existing law to the facts of digital evidence cases, such as the second hypothetical case involving Fred Felony's hack into the Smiths' computers. While the existing rules work well for physical evidence, they raise a number of puzzles when applied to digital evidence. Fitting the two-stage warrant process of digital evidence cases into the single-stage approach of existing law generates four distinct problems: defining the evidence to be seized; defining the place to be searched; regulating the timing of the warrant process; and facilitating judicial review of the warrant process.

### A. What is the Evidence to Be Seized?

Consider the first puzzle: how can investigators draft the warrant so that it particularly describes the "things to be seized?" It is a basic tenet of Fourth Amendment law that the "thing to be seized" named in the warrant is the item that the police have probable cause to believe constitutes evidence, a fruit or instrumentality of crime, or contraband. If a piece of computer hardware is known to be contraband or an instrumentality of crime, this tenet may be easy to satisfy. For example, a computer used to hack into another computer is an instrumentality of crime; likewise, a computer used to store child pornography is both an instrumentality of crime and contraband.[16] In these cases, the warrant can name the computer hardware itself. But what if the computer is merely a storage device for evidence, or the police do not know if a particular computer is in fact an instrumentality of crime or contraband? What should the warrant describe as the evidence to be seized?

There are two basic choices, corresponding to the two stages of the warrant process for digital evidence. The first choice is to describe the evidence to be seized as the physical storage devices — the computers themselves. Of course, investigators will not know exactly what those computers look like before they execute the search. In Fred Felony's case, for example, the most specific description the police likely could use would be something like "any computers, computer equipment, diskettes, CD-ROMS, or other electronic storage devices." While not terribly particular, this approach does describe accurately the evidence to be seized in the initial physical search. If you focus on that initial stage, the warrant will be accurate; the police will execute the warrant by entering the place to be searched and looking for (and then retrieving) the physical computers and other storage devices.

The second choice is to describe the evidence to be seized as the digital evidence itself – the electronic data. In the case of Fred Felony's hack, the warrant could state that it authorizes the seizure of "files containing the Mastercard number 2626 2727 2838 1812, or other evidence relating to Mr. and/or Mrs. John Smith of 123 Main Street." This approach does not describe accurately what the police will do on-site, but it does describe the evidence sought at the second stage of the warrant process—the off-site electronic search. If you focus on the latter stage instead of the former, the warrant will be accurate; a forensic expert will execute the warrant by looking through the computers for specific evidence.

---

[16] *See* U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS app. F at 198-217 (2000), *available at* http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf [hereinafter DOJ MANUAL].

Neither choice fits the traditional Fourth Amendment rules particularly well. Describing the things to be seized as the physical storage devices creates two problems. First, the warrant becomes overbroad. The police do not have probable cause to seize every computer storage device located on the premises. Rather, they have probable cause to believe that those computers contain some kind of digital evidence of the crime. Naming the items to be seized as the physical storage devices may be technically accurate at the first stage, but it also means that the warrant itself is no longer as particular as the scope of probable cause. Second, the warrant says nothing (either implicitly or explicitly) about the later search through the computer for the digital evidence. When the forensic experts look through the computer for evidence described in the warrant, they will have nothing to guide them. The warrant will merely say it authorizes the seizure of computer storage devices.

Equivalent problems arise if the warrant describes the particular files as the things to be seized. On one hand, this approach cures the overbreadth problem; the warrant is now much more particular. On the other hand, focusing on particularity creates a new problem. The warrant no longer describes accurately how the initial stage of the warrant will be executed. The warrant authorizes the search and seizure of specific files and data, but the investigators plan to seize all the hardware they can find on-site and send it to a lab for analysis. The execution of the warrant will no longer track what the warrant itself authorizes. Another technical problem is that copying a computer file does not actually "seize" it. As a result, the seizure that occurs is of the device holding the data rather than the data itself.[17] In effect, the police face a choice about what Fourth Amendment error they want to introduce. If they list the evidence to be seized as the physical device, then the warrant will be overbroad; if they list the evidence to be seized as the digital evidence, then the warrant no longer authorizes the police to do what they plan to do.

---

[17] *See* Kerr, *supra* note 8 (citing Arizona v. Hicks, 480 U.S. 321 (1987)).

### *B. What is the Place to be Searched?*

Although this issue arises less frequently, similar problems can arise when investigators attempt to describe the place to be searched. Digital evidence may be stored on a network or located inside an already seized computer stored in government custody. When either of these situations occur, the police may not need authorization to enter the place where the evidence is located. In such cases, what is the place to be searched?

In traditional cases, investigators simply list the location of the physical search as the location where the warrant will be executed. For example, if the police plan to search Fred Felony's apartment at 13 Prospect Avenue, Apartment A, they will list Fred's apartment as the place to be searched. However, this is only the location of the physical search, not the electronic search. In some cases, however, the latter may be more important. For example, a number of decided cases involve warrants authorizing the search of computers already seized and in law enforcement custody.[18] In these cases, the physical search and seizure has already occurred. The police already have the computer, and the warrant is needed only to authorize the electronic search. In such a case, how can the police satisfy the Fourth Amendment's requirement that the warrant specify the place to be searched? Should they list the place to be searched as the physical location of the storage device, such as "storage locker #7 in the Seventh Precinct?" Or, should they list the computer itself, such as "a Dell personal computer with Serial Number X10-23533"? The former satisfies the traditional need to specify the physical location of the search, but in a purely formalistic way; the latter is more accurate, but does not attempt to name a "place" to be searched.

The problem has particular importance in the case of data stored remotely on a computer network. Imagine that the police plan to execute a warrant to find a particular e-mail stored on a computer network by logging on to the network (or having an employee of the network operator do so) and retrieving the information remotely. Is the place to be searched the location of the police or the evidence? If the place to be searched is the location of the police when they log on to the network, police can engage in forum-shopping. Depending on how the network is configured, the police may be able to access it from anywhere. If the place is where the individual file is stored, on the other hand, it may stymie investigations. Investigators may be unable to know ahead of time where the evidence is located, and the retrieval of evidence may involve a search outside the United States where no warrant can be obtained.[19]

---

[18] *See, e.g.*, United States v. Gray, 78 F. Supp. 2d 524, 530-31 (E.D. Va. 1999) (involving a second warrant obtained to search a computer already in law enforcement custody).

### C. *When Can the Search be Executed?*

The third question concerns the timing of the second search. Statutory rules governing the warrant process generally lay out a specific time frame for executing the warrant. For example, Rule 41 states that the warrant must be executed "within a specified period of time no longer than 10 days"[20] after the warrant has been signed, and that the search must be executed only between the hours of 6:00 a.m. and 10:00 p.m.[21] It also states that the person who executes the warrant "must enter on its face the exact date and time it is executed."[22] These timing requirements appear reasonable and appropriate in the case of a search for physical evidence. The Rules ensure that Officers do not wait until the probable cause becomes stale, that they do not invade people's homes in the middle of the night, and that they leave a record of the exact time that the warrant was executed. The same requirements apply reasonably to the physical-search stage of the two-stage warrant process for physical evidence. But they leave open a question: what rules apply to the timing of the second stage, the electronic search?

---

[19] *Cf.* United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001) (remote search of Russian server from United States).

[20] FED R. CRIM. P. 41(e)(2)(A).

[21] *Id.* 41(a)(2)(B).

[22] *Id.* 41(f)(1).

The existing rule leaves open only two possibilities, neither of which is particularly appealing. The first possibility is that the timing requirements of Rule 41 also apply to the electronic search. Under this approach, the computer forensic process must be completed within ten days of the issuance of the warrant, and can be performed only between the hours of 6:00 a.m. and 10:00 p.m. This proves an impossible standard to meet in practice. As we saw in the hypothetical with Fred Felony's computers, the forensic process typically takes a number of days once started, and the backlog of cases in most jurisdictions means that weeks or months may pass before the analysis even begins. Nor does this approach make much sense. While it is desirable for electronic searches to occur quickly, staleness is not a concern after the container of evidence has been seized. In addition, there is no reason why a forensic examiner working in the laboratory at night has to stop at 10:00 p.m. or cannot come in to work before 6:00 a.m.[23]

However, the second possibility is also problematic. The electronic search process may simply be exempt from Rule 41's timing requirements. If Rule 41 is construed in this way, nothing requires government investigators to begin or complete the forensic analysis at any time. Investigators can take all of the target's computer equipment and hold them for months or even years, without even beginning the forensic process. This is particularly problematic given that some computers seized may not contain any evidence. In the hypothetical case of seizing Fred Felony's computer, the investigators found two computers and multiple additional storage devices. When the electronic search was executed months later, however, it turned out that only one of the computers contained evidence. This means that the other computer and storage devices ideally would not have been seized in the first place; a rule allowing the police to hold a target's computer until they get around to searching it (however long that may be) seems unfairly insensitive to the legitimate needs of computer owners. The existing Rule 41 is simply ill-prepared to handle the two-stage search process of digital evidence cases, as it forces the second step either to fit within the rules of the first or follow none at all.

---

[23] That is, other than the Fair Labor Standards Act of 1938, 29 U.S.C. § 207 (2000).

### *D. What are the Oversight and Record-keeping Requirements, and When Must Property be Returned?*

The final issues involve oversight and review of the warrant process, and include the rules that govern when seized property must be returned. Traditional rules require the officer who executes the warrant to create an inventory of the items seized and to provide the judge the inventory list of property seized.[24] The rules then place a burden on the aggrieved property owner to file a motion in court for return of the property.[25] Under Rule 41, the court generally will order the return of the property only if the police no longer have a legitimate claim that they need it for an investigation.[26]

These rules prove awkward in the case of digital evidence searches. First, it is unclear whether the record-keeping requirements refer only to the initial physical search or also include the subsequent electronic search. For example, should the required inventory list include only the physical evidence taken at the first stage, or should it include a list of the computer programs and files that the computers are later revealed to contain? Requiring investigators to generate a quick analysis of the files is impractical given the time-consuming nature of the forensic process; further, owners of computer equipment ordinarily should know what files their computers contain and should not need the police to tell them. If the inventory relates only to the physical evidence, however, then the existing rules do not require any record-keeping for the subsequent electronic search. Once again, applying the initial search rules to the electronic search proves difficult, while declining to apply them leaves an important step of the warrant process unregulated. Similarly, who should receive the inventory list in the case of a computer already in government custody? If the government has a computer in its custody and obtains a warrant to search it, does it need to find the owner of the computer and serve the inventory list on the owner?

---

[24] *See* FED. R. CRIM. P. 41(f)(4).

[25] *Id.* 41(g).

[26] *See infra* note 116.

The second difficulty concerns the return of property. Computer searches often require investigators to seize all of the computers and storage devices that they find on-site and remove them for subsequent analysis. In many cases, only some of those computers and storage devices will actually contain evidence of the crime; in some cases, none of them will. We saw this problem in the Fred Felony hypothetical. When the investigator entered Fred's apartment, he found several computers and did not know which one contained the evidence he needed. As noted earlier, the investigators often will not realize which computers contain the necessary evidence until many months later when the computers are finally analyzed. Under the current version of Rule 41, however, a property owner simply must wait until the government gets around to looking at the computer. Existing rules simply were not designed for a two-step search environment that begins with a broad seizure. As a result, the rules show little attention to the needs of property owners who may need equipment back for reasons unrelated to the investigation.

## III. EXISTING LAW APPLYING THE WARRANT PROCESS TO SEARCHES FOR DIGITAL EVIDENCE

Courts have provided tentative answers to two-and-a-half of the four puzzles raised by the application of the warrant process rules to searches for digital evidence. The one puzzle that has not been addressed at all is how to define the "place to be searched." This issue simply has not yet come up in litigation. Also, only a small amount of litigation has focused on the record-keeping requirements and the rules governing the return of seized computers. Two other steps have been the subject of extensive litigation. The most frequently litigated issue relates to how to describe the evidence to be seized. In the last three years, there has also been a growing body of caselaw on the timing of the search. This section reviews the existing caselaw in order to frame the normative reform proposals that will be made in Part IV.

### *A. The Things to be Seized*

Courts generally have deferred to the government's choice of whether to describe the property to be seized as the computer hardware or the digital evidence itself. Both approaches have been upheld, at least within limits; no court has required that the police use one approach or the other. This does not mean that courts have rubber-stamped the government's work. Rather, they have scrutinized both approaches and concluded that, within reason, the government can chose which approach to use. The courts' approval of both strategies owes in large part to a practice followed by many investigators (and recommended by the Department of Justice) of explaining the need for the two-stage search process in the warrant affidavit. This practice uses the affidavit as a way to communicate the details of the search process to the judge; by signing the warrant, the court in effect approves the two-step search process. At least some courts have suggested that this practice effectively cures what otherwise could be an inherent constitutional defect in the two-stage search for digital evidence.

The more common practice has been to describe the evidence to be seized as the physical computers. An example of a decision upholding such a practice is *United States v. Upham*.[27] In *Upham*, agents investigating a child pornography case obtained a warrant to seize "[a]ny and all computer software and hardware, . . . computer disks, [and] disk drives."[28] Judge Boudin rejected the defendant's claim that the seizure of

---

[27] 168 F.3d 532 (1st Cir. 1999).

[28] *Id.* at 535. The warrant in *Upham* also named the evidence itself: "[a]ny and all visual depictions, in any format or media, of minors engaging in sexually explicit conduct [as defined by the statute]." *Id.* However, the court resolved the challenge, by relying only on the first description. *Id.* at 536.

"all computers" was overbroad:

> As a practical matter, the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the images. A sufficient chance of finding some needles in the computer haystack was established by the probable-cause showing in the warrant application; and a search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for a weapon or drugs. We conclude, as did the Ninth Circuit in somewhat similar circumstances, that the . . . [language] was not unconstitutionally overbroad.
>
> Of course, if the images themselves could have been easily obtained through an on-site inspection, there might have been no justification for allowing the seizure of *all* computer equipment, a category potentially including equipment that contained no images and had no connection to the crime. But it is no easy task to search a well-laden hard drive by going through all of the information it contains, let alone to search through it and the disks for information that may have been "deleted." The record shows that the mechanics of the search for images later performed off site could not readily have been done on the spot.[29]

Note that Judge Boudin looked to the practical needs of law enforcement to determine whether the warrant was overbroad, rather than to the scope of probable cause. Because the government had made the case that it needed to seize all computers for practical reasons, it was not overbroad for the warrant to reflect this on its face.[30]

The willingness to approve seizures of equipment in many cases may owe in part to the fact that many of the existing cases involve computers used to store child pornography or, more rarely, obscenity. In such a case, the computer hardware itself technically is an instrumentality of crime and forfeitable.[31] As a result, seizure of the contraband equipment is legal even if some of the files contained in the equipment do not relate to the crime. The Tenth Circuit made this point explicitly in the case of *Davis v. Gracey*, which involved a warrant to seize equipment that contained obscenity.[32] The police seized two computer servers used to provide e-mail and digital images to about two thousand subscribers.[33] After the equipment was seized, its owners brought a civil action claiming that the seizure violated the Fourth Amendment.[34] In particular, the plaintiffs claimed that the seizure was overbroad because it seized a great deal of innocent material.[35] The court rejected this argument because the equipment was contraband that could be seized:

---

[29] *Id.* at 535 (citations omitted).

[30] *Id.*

> In the typical case, the probable cause supporting seizure of a container is probable cause to believe that the container's contents include contraband or evidentiary material. Here, in contrast, the probable cause supporting the seizure of the computer/container related to the function of the computer equipment in distributing and displaying pornographic images, not to its function in holding the stored files. The fact that a given object may be used for multiple purposes, one licit and one illicit, does not invalidate the seizure of the object when supported by probable cause and a valid warrant.[36]

Even in *Gracey*, however, the court was influenced by the practical difficulties inherent in a contrary rule requiring the police to distinguish between the seizure of computer equipment and the seizure of individual files stored inside. The court explained:

> We . . . note the obvious difficulties attendant in separating the contents of electronic storage from the computer hardware during the course of a search. Perhaps cognizant of the

---

[31] *See* DOJ MANUAL, *supra* note 16, at 206.

[32] 111 F.3d 1472, 1475-76 (10th Cir. 1997).

[33] *Id.*

[34] *Id.* at 1476.

[35] *Id.*

[36] *Id.* at 1480.

> potential burdens of equipment, expertise, and time required to access, copy, or remove stored computer files, plaintiffs have not suggested any workable rule. In short, we can find no legal or practical basis for requiring officers to avoid seizing a computer's contents in order to preserve the legality of the seizure of the computer hardware.
>
> . . . Even in the typical case, seizure of a container need not be supported by probable cause to believe that *all* of the contents of the container are contraband. The seizure of a container is not invalidated by the probability that some part of its "innocent" contents will be temporarily detained without independent probable cause. We will not hold unlawful the otherwise constitutional seizure of the computer equipment in order to prevent the temporary deprivation of plaintiffs' rights to the contents.[37]

In some cases, however, warrants that listed only the physical property seized during the physical search have been found inadequate because they failed to provide sufficient guidance to regulate the search at the electronic stage. The most important example is *United States v. Riccardi*.[38] In *Riccardi*, the police executed a warrant to seize material relating to child pornography from the defendant's home.[39] During the initial search, they saw that the defendant had a computer.[40] The agents applied for a second warrant to allow them to go back and seize the target's computer.[41] The second warrant listed the items to be seized as the target's computer,

> and all electronic and magnetic media stored therein, together with all storage devises [sic], internal or external to the computer or computer system, including but not limited to floppy disks, diskettes, hard disks, magnetic tapes, removable media drives, optical media such as CD–ROM, printers, modems, and any other electronic or magnetic devises used as a peripheral to the computer or computer system, and all electron-

---

[37] *Id.* at 1480-81 (citations omitted).

[38] 405 F.3d 852 (10th Cir. 2005).

[39] *Id.* at 858.

[40] *Id.*

[41] *Id.*

ic media stored within such devises.[42]

The warrant did not explain that it was limited to computers used to store child pornography.[43] In an opinion by Judge McConnell, the court held that the warrant was insufficiently particular because it failed to give the police sufficient guidance as to what kind of evidence they could search for during the forensic analysis.[44] "By its terms, the warrant thus permitted the officers to search for anything—from child pornography to tax returns to private correspondence. It seemed to authorize precisely the kind of 'wide-ranging exploratory search[] that the Framers intended to prohibit.'"[45] If the warrant had explained the type of evidence that the police were looking for, McConnell suggested, then it would have been sufficiently particular.[46] The inclusion of the type of evidence was not necessary at the initial physical stage because the police could not know which computers actually did store the evidence sought, but was needed at the second electronic stage to limit the search that the forensic specialists conducted.

*United States v. Hunter*[47] is somewhat similar. In *Hunter*, investigators searched an attorney's office for evidence that he had helped a client launder money.[48] The warrant authorized the seizure of "[a]ll computers . . . [a]ll computer storage devices . . . [and a]ll computer software systems."[49] The district judge found that this description was overbroad because it did not mention "the specific crimes for which the equipment was sought" or incorporate by reference the affidavit's discussion of the search strategy that investigators planned to use in order to avoid interfering with innocuous files protected by the attorney-client privilege.[50] Without this information, the court suggested, the warrant did not provide sufficient guidance to the officers.[51] As in *Ricardi*, however, the court did not suppress the evidence on the ground that the overall care that the officers showed in planning and conducting the search made the "good faith" exception applicable.[52]

---

[42] *Id.* at 862.

[43] *Id.*

[44] *Id.* at 863.

[45] *Id.* at 863 (alteration in quoted text) (quoting Maryland v. Garrison, 480 U.S. 79, 84 (1987)). The court admitted the evidence, however, on the ground that it satisfied the good faith standard. *Id.* at 864.

[46] *Id.* at 863.

[47] 13 F. Supp. 2d 574.

[48] *Id.* at 578.

[49] *Id.* at 584 (citation omitted).

Another notable case rejecting a computer warrant as insufficiently particular is a civil decision, *Arkansas Chronicle v. Easley*.[53] In *Easley*, state investigators obtained a warrant to search a journalist's home for evidence relating to the Oklahoma City bombings.[54] The investigators sought a video and three still photographs believed to be located on the journalist's computer.[55] Instead of describing the property to be seized as the video and the photographs, the warrant focused only on the physical stage of the search: the warrant permitted the agents to seize "[a]ny and all computer equipment, hard disk drives, compact disks, floppy disks, magnetic tapes or other magnetic or optical media capable of storing information in an electronic, magnetic or optical format."[56] As in *Riccardi*, the warrant was held invalid on the ground that it did not limit the scope of the electronic search: "In these circumstances, such a warrant essentially amounted to a general warrant giving police the authority to rummage through every single computer file and document with no limitations on which documents could be seized."[57] Judge Ellis also expressed concern that the warrant was too broad in terms of limiting the seizure at the initial physical stage, a problem made more severe by the fact that the role of the computer in the case was mere evidence rather than contraband or an instrumentality of crime.[58]

---

[50] *Id.*; *see also* United States v. Clough, 46 F. Supp. 2d 84, 87 (D. Me. 2003) (finding computer warrant unconstitutionally broad when it permitted the seizure of "text documents of any variety, including e-mail, websites, records of chat sessions, correspondence or shipping records; and . . . digital images of any variety, including still images and videos" without additional limitation) (citation omitted).

[51] *Hunter*, 13 F. Supp. 2d at 584.

[52] *Id.* at 584-85.

[53] 321 F. Supp. 2d 776 (E.D. Va. 2004) (Ellis, J.).

[54] *Id.* at 778.

[55] *Id.* at 793.

[56] *Id.* at 792.

[57] *Id.* at 793 (citation omitted).

Warrants that list the evidence to be seized as the information sought are less common than warrants that list the evidence to be seized as the physical storage device. Nonetheless, warrants in such cases have been upheld as well.[59] In these cases, the defense challenge generally shifts ground: instead of arguing that the warrant was overbroad, defendants claim that the execution of the warrant was in "flagrant disregard" of the warrant.[60] The "flagrant disregard" standard has been adopted by the courts of appeal to review the execution of a warrant;[61] if the evidence in question was within the scope of the warrant, that evidence is suppressed only if the search so grossly exceeds the scope of the warrant during execution that the authorized search appears to be merely a pretext for a "fishing expedition" through the target's private property.

This is a very difficult standard for defendants to satisfy, as it amounts to a requirement of large-scale bad faith. Proving bad faith is difficult in light of the significant body of caselaw in recent years emphasizing the practical reasons investigators may need to seize computers and subject them to an off-site search. Searching on-site for the evidence can be more disruptive than searching on-site; courts have found it "obvious" that searching a computer for evidence requires great skill, time and expertise.[62] In light of that it is generally more reasonable to allow officers to search off-site than park at the suspect's home for a few days while the search of his computer occurs.[63]

---

[58] *Id.*

[59] *See, e.g.,* United States v. Gawrysiak, 972 F. Supp. 853, 866-67 (D.N.J. 1997).

[60] *See, e.g.,* United States v. Liu, 239 F.3d 138, 140 (2d Cir. 2000); United States v. Foster, 100 F.3d 846, 849 (10th Cir. 1996); *Gawrysiak*, 972 F. Supp. at 864.

[61] *See, e.g., Liu*, 239 F.3d at 140; *Foster*, 100 F.3d at 851; United States v. Young, 877 F.2d 1099, 1105-06 (1st Cir. 1989). Notably, the Supreme Court has not addressed this issue directly.

[62] Davis v. Gracey, 111 F.3d 1472, 1480 (10th Cir. 1997) (noting "the obvious difficulties attendant in separating the contents of electronic storage [sought as evidence] from the computer hardware [seized] during the course of a search.").

[63] United States v. Henson, 848 F.2d 1374, 1383-84 (6th Cir. 1988) ("We do

As one district judge noted, "[t]he Fourth Amendment's mandate of reasonableness does not require the agent to spend days at the site viewing the computer screens to determine precisely which documents may be copied within the scope of the warrant."[64] These precedents make it difficult to establish that a routine computer search was in "flagrant disregard" of the warrant.

The judicial focus on practical reasons why a warrant must be executed in a particular way has led to a new practice among prosecutors and law enforcement agents in the case of digital evidence searches. In traditional cases, the affidavit in support of the warrant explains the officer's probable cause to believe that evidence described in the warrant will be located in the place searched. In digital evidence warrants the affidavit is used to do much more. In many cases, the affidavit is used to explain the need for a two-step search to the magistrate judge. The affidavit informs the judge of what investigators plan to do when they execute the warrant, explaining the practical needs that they believe justify the two-step search process. The magistrate's decision to sign the warrant in effect "approves" the two-stage search ex ante.[65] With the search process approved before the search is executed, a defendant will have a hard time arguing that the search was executed in "flagrant disregard" of the warrant or that it was overbroad.

The idea of justifying the overbroad seizure through language in the affidavit derives in part from an early Ninth Circuit case involving paper documents, *United States v. Tamura*.[66] In *Tamura*, the government seized boxes of documents and took them offsite for review. The boxes contained some documents which were evidence of crime commingled

---

not think it is reasonable to have required the officers to sift through the large mass of documents and computer files found in the [defendant's] office, in an effort to segregate those few papers that were outside the warrant.") (citation omitted).

[64] *Gawrysiak*, 972 F. Supp. at 866.

[65] *Cf.* United States v. Hay, 231 F.3d 630, 634 (9th Cir. 2000) (upholding magistrate's authorization to both seize and search a computer).

[66] 694 F.2d 591, 594-95 (9th Cir. 1982).

with innocuous documents, and the government seized all of them because of the infeasibility to search through all boxes on site.[67] In an opinion by Judge Fletcher, the Ninth Circuit offered a suggestion for how the government could "generally . . . avoid violating [F]ourth [A]mendment rights" in cases involving commingled documents: get prior permission to seize all of the documents and conduct an off-site search before actually doing so, in order that "wholesale removal" is "monitored by the judgment of a neutral, detached magistrate."[68] In other words, judges should sign off on the wholesale seizure of documents so overbroad seizures are not conducted unless they are required by practical concerns.[69]

The Justice Department has recommended something akin to the *Tamura* approach in its manual on *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*.[70] The DOJ Manual recommends the following practice when the physical storage device is only a storage container for evidence:

> The affidavit should . . . contain a careful explanation of the agents' search strategy, as well as a discussion of any practical or legal concerns that govern how the search will be executed. Such an explanation is particularly important when practical considerations may require that agents seize computer hardware and search it off-site when that hardware is only a storage device for evidence of crime. Similarly, searches for computer evidence in sensitive environments (such as functioning businesses) may require that the agents adopt an incremental approach designed to minimize the intrusiveness of the search. The affidavit should explain the agents' approach in sufficient detail that the explanation provides a useful guide for the search team and any reviewing court. It is a good practice to include a copy of the

---

[67] *Id.* at 595.

[68] *Id.* at 595-96.

[69] *Id.* at 596.

[70] DOJ MANUAL, *supra* note 16, at 70, 72. In the interest of full disclosure, I should note that I wrote this manual under the auspices and with the guidance of others at the Department of Justice.

> search strategy as an attachment to the warrant, especially when the affidavit is placed under seal.[71]

Exactly what kind of detail is required in the affidavit presently remains an open question. As I explain in another article, a few courts have indicated that the search strategy should include the specific steps that will be undertaken when the forensic analyst conducts the electronic search.[72] That is, the affidavit should not only explain the need for a two-stage search, but should actually provide a detailed list of the steps that will be taken during the second stage. As I argue elsewhere, it is my view that such detail should not be required, especially ex ante, and that the reasonableness of the electronic search should be reviewed ex post using the same "flagrant disregard" standard used in physical searches.[73] But the present uncertainty of how much detail an affidavit should include does not alter the broad acceptance of the basic strategy: prosecutors can "cure" any defect caused by the two-stage warrant process by explaining the process in the affidavit. By signing the warrant, the judge in effect approves the two-stage search and cures what otherwise would be a technical defect raised by trying to force a two-stage process into a legal rule designed to handle a single-stage search.

### *B. When Can the Search be Executed?*

The last five years have witnessed a considerable amount of litigation—not to mention a great deal of informal negotiations between prosecutors and magistrate judges—on when a search for digital evidence can be executed. The legal issues fall into two basic categories. The first set of issues concerns whether the timing restrictions of warrant rules such as Rule 41 apply to the subsequent electronic search. The second set of issues concerns the legality and propriety of judicially-imposed restrictions on the timing of the electronic search process. The first questions have a reasonably clear answer. The second do not.

---

[71] *Id.* at 219.

[72] Kerr, *supra* note 8.

[73] *Id.*

The few courts that have addressed the first issue have held that statutory rules requiring the search to occur within a particular time window do not apply to the computer forensic process. For example, in *Commonwealth v Ellis*,[74] investigators seized a computer server at a law firm.[75] The defendant relied on a state supreme court decision that had interpreted the state warrant law to require that every search pursuant to a warrant must be completed within seven days of the warrant being issued. The *Ellis* court concluded that this did not apply to the computer forensic process.[76] According to the Court:

> [the state supreme court's interpretation of state law] was made before the advent of the computer age, and before the Supreme Judicial Court could envision a scenario where execution of a search could continue after the return of the warrant had been filed. And where computers are seized, that is precisely what occurs. . . . Courts have recognized that the search of computer data involves more preparation than an ordinary search and a greater degree of care in the execution of the warrant; and that the search may involve much more information. As such, computer searches are not, and cannot be, subject to the statutory requirement that the search be completed within seven days.[77]

Federal courts have reached the same conclusion in the context of interpreting the ten-day rule of Rule 41, which requires warrants to be executed within ten days of being signed. A handful of federal district courts have addressed the issue and held that the computer forensic process is not included within the ten day rule.[78] As one court explained in *United*

---

[74] 10 Mass. L. Rptr. 464, 1999 Mass. Super. LEXIS 368 (Mass. Super. Ct. 1999).

[75] *Id.*

[76] *Id.*

[77] *Id.* at *29-*30 (footnote and citations omitted).

[78] United States v. Gorrell, 360 F. Supp. 2d 48, 55 n.5 (D.D.C. 2004) ("The warrant did not limit the amount of time in which the government was required to complete its off-site forensic analysis of the seized items and the courts have

*States v. Hernandez*:

> Neither Fed. R. Crim. P. 41 nor the Fourth Amendment provides for a specific time limit in which a computer may undergo a government forensic examination after it has been seized pursuant to a search warrant. In most cases the forensic examination of the computer will take place at a different location than that where the computer was seized. The same principle applies when a search warrant is performed for documents. The documents are seized within the time frame established in the warrant but examination of these documents may take a longer time, and extensions or additional warrants are not required. The examination of these items at a later date does not make the evidence suppressible.[79]

The more difficult questions concern the second set of issues. First, are there any constitutional limits on when the electronic search must occur? Second, do magistrate judges have the statutory authority to condition the issuance of the warrant on the government's agreement to conduct the electronic search in a particular period of time? Two federal district courts have recently suggested that the Fourth Amendment's reasonableness standard requires the investigators to search the computer for the evidence before too much time has elapsed. The apparent idea is that an excessive delay before the second search renders the continued seizure unreasonable, requiring suppression of the evidence as fruit of an unreasonable seizure.[80]

The first of the two cases is *United States v. Grimmett*.[81] In *Grimmett*, officers seized computers pursuant to a state war-

---

not imposed such a prophylactic constraint on law enforcement."); United States v. Hernandez, 183 F. Supp. 2d 468, 480 (D.P.R. 2002) (stating that Rule 41 does not "provide[] for a specific time limit in which a computer may undergo a government forensic examination after it has been seized pursuant to a search warrant."); United States v. Crim. Triumph Capital Group, 211 F.R.D. 31, 66 (D. Conn. 2002); United States v. Habershaw, 2001 WL 1867803, at *8 (D. Mass. May 13, 2001).

[79] *Hernandez*, 183 F. Supp. 2d at 480.

[80] *See Ellis*, 10 Mass. L. Rptr. at *29.

[81] 2004 WL 3171788 (D. Kan. 2005).

rant that authorized a search for child pornography.[82] State law gave the officers ninety-six hours to execute the search.[83] The officers seized the computers from the defendant's home within the ninety-six-hour window, but then a few weeks passed before the government's computer expert searched the computer for child pornography.[84] The defendant claimed that the failure to search the computer for evidence within the ninety-six-hour window violated the Fourth Amendment.[85] The court rejected the claim, but did accept the basic idea that the timing of the computer search was governed by a reasonableness analysis:

> The conduct of law enforcement officers in executing a search warrant is governed by the Fourth Amendment's mandate of reasonableness. The Fourth Amendment does not provide a specific time in which a computer may be subjected to a government forensic examination after it has been seized pursuant to a search warrant. The court finds that the Fourth Amendment requires only that the subsequent search of the computer be made within a reasonable time . . . . The court finds that the subsequent search was conducted within a reasonable time since it was concluded within a few weeks of the execution of the warrant.[86]

The second case is *United States v. Syphers*.[87] The *Syphers* court held that a seven month delay in the forensic analysis of a computer was reasonable because it was justified by legitimate practical needs:

> Syphers asserts that the state acted unreasonably in detaining the CPU for seven months before completing the search. The government counters that the Fourth Amendment does

---

[82] *Id.* at *1-*2.

[83] *Id.* at *1.

[84] *Id.* at *2.

[85] *Id.* at *3.

[86] *Id.* at *5 (citation omitted).

[87] 296 F. Supp. 2d 50 (D.N.H. 2003), *aff'd*, 2005 U.S. App. LEXIS 22527 (1st Cir. 2005) (the First Circuit affirmed, but relied on circuit precedent that did not directly address reasonableness).

> not impose any limitation on the length of a forensic examination of a computer. "However, from the general prohibition against 'unreasonable searches and seizures' . . . it may be contended that there are some constitutional limitations upon the time when a search warrant may be executed." . . .
>
> Based on the same reasons which support the finding that the state acted in good faith with respect to the warrant, the court concludes that the state did not overstep any constitutional boundaries in seizing the CPU for seven months under the circumstances presented.[88]

The *Syphers* court then cited a military court decision by the U.S. Navy-Marine Corps Court of Criminal Appeals in *United States v. Greene*.[89] In *Greene*, Special Agents of the Naval Criminal Investigatory Service (NCIS) obtained the target's consent to seize and search the suspect's computer for child pornography.[90] The consent form did not state the length of time that Greene agreed to allow the NCIS to seize his computer, but three months elapsed before the forensic process was undertaken.[91] The court concluded that the three month delay was not unreasonable:

> While the appellee did not expressly consent to a period of 3 months of NCIS seizure and retention of his property, the plain language of the consent form clearly states he agreed to allow the investigators to remove and retain his property for investigative purposes. In other words, the appellee consented to a seizure of his property. If the appellee believed that retention for 3 months was unreasonable, he never said so. We hold that, in this case, the consensual seizure and subsequent retention for 3 months was not unreasonable.[92]

In a footnote, however, the court warned that there were limits to when the search could be completed:

---

[88] *Id.* at 59 (citation omitted).

[89] 56 M.J. 817 (N-M. Ct. Crim. App. 2002).

[90] *Id.* at 820.

[91] *Id.* at 821-23.

[92] *Id.* at 823.

> Although we hold that 3 months is constitutionally permissible here, we also believe that an excessively long period of retention, following a lawful seizure, could be unreasonable. We decline to try to draw a "bright-line" that would apply in all circumstances. Each case must be considered on its own facts.[93]

While *Grimmett*, *Syphers* and *Greene* suggest that an excessive delay in the forensic process may render the seizure unreasonable, it is unclear whether this suggestion makes sense in light of existing law. First, the computers in all three cases were instrumentalities of the crime: they were used to possess illegal images of child pornography. Given that these items are forfeitable, it makes little sense to suggest that continued deprivation of the property renders the seizure unreasonable. Second, statements by prior courts and commentators that delay in the timing of a search may have constitutional limitations were made in the context of an initial physical search. In those circumstances, delay may allow the probable cause to become stale. The search is unreasonable because as time passes the case for probable cause begins to evaporate. In contrast, a seized computer stores its information permanently. The initial physical search and seizure has already occurred. The cause can no longer become stale.

Whether the framework suggested in *Grimmett*, *Syphers* and *Greene* will be adopted by other courts remains unclear. A large body of case law indicates that the amount of time that property or a person is seized factors into the reasonableness of the seizure.[94] Courts could therefore hold that a warrant authorizes a theoretically overbroad computer seizure, but that as time passes the overbroad seizure becomes less reasonable. One difficulty with this approach is that the vague standard gives little guidance to law enforcement. Most agents and prosecutors are at the mercy of forensic lab employees with regard to the timing of the electronic search. The timing of a search may be determined by the lab's resources, the forensic analyst's skills, the specific tools the lab uses, and the type of investigation. A general reasonableness requirement does not provide clear guidance to law enforcement and may end up punishing agents and prosecutors for factors beyond their control. A better approach would be to provide clear guidance using statutory warrant rules.

---

[93] *Id.* at n.4.

[94] *See, e.g.,* United States v. Place, 462 U.S. 696, 703 (1983).

A related issue is whether magistrate judges have the statutory authority to condition the issuance of a warrant on the government's agreement to search the computers, or at least begin the search, within a specific period of time. As the DOJ Manual explains:

> Several magistrate judges have refused to sign search warrants authorizing the seizure of computers unless the government conducts the forensic examination in a short period of time, such as thirty days. Some magistrate judges have imposed time limits as short as seven days, and several have imposed specific time limits when agents apply for a warrant to seize computers from operating businesses. In support of these limitations, a few magistrate judges have expressed their concern that it might be constitutionally "unreasonable" under the Fourth Amendment for the government to deprive individuals of their computers for more than a short period of time.[95]

Do magistrate judges have the power to do this? The text of Rule 41 is not entirely clear, but suggests that judges may not. Rule 41(d)(1) is phrased as a command: "a magistrate judge . . . *must* issue the warrant if there is probable cause."[96] The rule appears to give the judge no power to withhold the warrant unless the government agrees to a special condition. As the DOJ Manual explains:

> the relevant case law is sparse, [but] it suggests that magistrate judges lack the legal authority to refuse to issue search warrants on the ground that they believe that the agents

---

[95] DOJ MANUAL, *supra* note 16, at 77.

[96] FED. R. CRIM. P. 41(d)(1) (emphasis added).

> may, in the future, execute the warrants in an unconstitutional fashion. *See* Abraham S. Goldstein, *The Search Warrant, the Magistrate, and Judicial Review*, 62 N.Y.U. L. REV. 1173, 1196 (1987) ("The few cases on [whether a magistrate judge can refuse to issue a warrant on the ground that the search may be executed unconstitutionally] hold that a judge has a 'ministerial' duty to issue a warrant after 'probable cause' has been established."); *In re Worksite Inspection of Quality Prod., Inc.*, 592 F.2d 611, 613 (1st Cir. 1979) (noting thel imited role of magistrate judges in issuing search warrants). As the Supreme Court suggested in one early case, the proper course is for the magistrate to issue the warrant so long as probable cause exists, and then to permit the parties to litigate the constitutional issues afterwards. *See Ex Parte United States*, 287 U.S. 241, 250 (1932) ("The refusal of the trial court to issue a warrant . . . is, in reality and effect, a refusal to permit the case to come to a hearing upone ither questions of law or fact and falls little short of a refusal to permit the enforcement of the law.").[97]

There are other perspectives, however. Susan Brenner and Barbara Frederiksen have argued that Rule 41 creates a "reservoir of inherent power" to place time restrictions on the computer forensic process.[98] They note that courts have allowed federal judges to issue anticipatory warrants that are triggered when some future event happens.[99] For example, the police can obtain a warrant to search a house the moment a suspicious package is delivered and can condition the execution of the warrant on the arrival of the suspicious package at the location to be searched. Brenner and Frederiksen suggest that restrictions on the timing of the computer forensic process are similar and thus implicitly allowed by Rule 41.[100]

I am not sure I am convinced by this argument. Anticipatory warrants are generally justified by the timing of probable cause. The thinking is that probable cause to execute the search is contingent on the condition precedent, such as the arrival of the package, occurring.[101] The warrant can be executed only when the condition precedent occurs because until that point, no probable cause exists and no warrant can issue unless probable cause exists. Further, Rule 41 has been amended specifically to allow for anticipatory warrants.[102] In light of these differences, I do not see how the power to issue anticipatory warrants implies the power to control the timing of the computer forensic process. Making a police officer wait to execute a warrant until there is probable cause seems quite different from making an officer conduct a forensic analysis of a seized computer within a specific window of time. In any event, the magistrate's power to impose time limits on the forensic process presently remains unclear.[103]

---

[97] DOJ MANUAL, *supra* note 16, at 77-78.

[98] Brenner & Frederiksen, *supra* note 4, at 114.

[99] *Id.*

[100] *Id.*

As a practical matter, agents will have little choice but to follow time limits on the forensic process when judges decide to impose them. In *United States v. Brunette*,[104] a magistrate judge allowed agents to seize the computers of a child pornography suspect, but added the condition that the forensic analysis must occur "within 30 days."[105] The agents seized two computers when they executed the search five days later.[106] A few days before the thirty-day period elapsed, agents obtained a thirty-day extension for review.[107] They examined one of the seized computers within the thirty-day extension period and found pornographic images of children.[108] However, the agents did not begin the review of the last computer until shortly after the extension period had elapsed.[109] Brunette argued that the evidence located on the last computer had to be suppressed because the search outside of the sixty-day period violated the terms of the judge's order.[110] The district court agreed, concluding that the failure "to adhere to the requirements of the search warrant and subsequent order" meant that "any evidence gathered from the . . . computer is suppressed."[111]

---

[101] *See, e.g.*, United States v. Grubbs, 377 F.3d 1072, 1077-78 (9th Cir.), *reh'g denied*, 389 F.3d 1306 (9th Cir. 2004), *cert. granted*, 74 U.S.L.W. 3199 (U.S. Sept. 27, 2005).

[102] United States v. Tagbering, 985 F.2d 946, 949 n.3 (8th Cir. 1993) (noting that a 1990 amendment to Rule 41(a)(1) "permits anticipatory warrants" (quoting FED. R. CRIM. P. 41 advisory committee's note (1990 amendments))); *see also* FED. R. CRIM. P. 41(b)(2) ("[A] magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed").

[103] *See also West End*, 321 F. Supp. 2d at 961 (holding that the magistrate has the power to require the submission of search protocol to fulfill the requirements of particularity and probable cause before a computer can be searched pursuant to a warrant).

[104] 76 F. Supp. 2d 30 (D. Me. 1999), *aff'd*, 256 F.3d 14 (1st Cir. 2001).

[105] *Id.*

[106] *Id.*

### C. *What Are the Oversight and Record-keeping Requirements, and When Must Property be Returned?*

Finally, a few courts have touched on the record-keeping requirements of statutory warrant rules and the return of seized computers. The thrust of the caselaw on record-keeping requirements is that they do not apply to the data. For example, the return on the warrant is limited to the physical property taken.[112] The federal rule requires notice, but that notice need only be of the "property taken," which presumably applies only to the physical equipment.[113] This is a sensible approach. The purpose of leaving a return is to inform the suspect of what property was taken, and this is best done by leaving a report of the physical property seized. After all, the suspect himself will know better than the police what files the storage device contains. It does not serve any interest of the warrant rules to require the police to search the computer, catalog its contents, and then notify the ower of what data resides on his hard drive.

---

[107] *Id.*

[108] *Brunette*, 256 F.3d at 16.

[109] *Brunette*, 76 F. Supp. 2d at 42.

[110] *Id.*

[111] *Id.*

[112] *See Ellis*, 10 Mass. L. Rptr. at *9 (holding that the search of the files stored on the computer did not have to be finished within the time period required for return of the warrant).

[113] United States v. Simons, 206 F.3d 392, 403 (4th Cir. 2000).

The caselaw on the return of physical property treats computers essentially like any other property. The basic rule is that if the government has a continuing need for the property, it can continue to hold it. As the DOJ Manual explains, this standard allows the government to hold on to seized computers throughout the forensic process:

> Rule 41(e) motions requesting the return of properly seized computer equipment succeed only rarely. First, courts will usually decline to exercise jurisdiction over the motion if the government has offered the property owner an electronic copy of the seized computer files.
>
> Second, courts that reach the merits generally find that the government's interest in the computer equipment outweighs the defendant's so long as a criminal prosecution or forfeiture proceeding is in the works. If the government does not plan to use the computers in further proceedings, however, the computer equipment must be returned. Further, a court may grant a Rule 41(e) motion if the defendant cannot operate his business without the seized computer equipment and the government can work equally well from a copy of the seized files.[114]

Notably, the current rule does not provide any mechanism to allow a suspect to get a copy of seized files unrelated to the investigation. While investigators may decide to generate copies of particular files on their own for suspects, no legal rule requires it.[115]

---

[114] DOJ MANUAL, *supra* note 16, at 81 (citations omitted).

[115] *Id.* The DOJ Manual recommends that agents should return "innocent files" to suspects if the suspects can show a "legitimate need" for the files or hardware and the agents can return the files "without either jeopardizing the investigation or imposing prohibitive costs on the government." *Id.* at 77 n.13.

## IV. RETHINKING THE WARRANT PROCESS IN AN AGE OF DIGITAL EVIDENCE

What is the future of the warrant process? This section proposes a series of changes to the law governing the warrant process to update it for the era of digital evidence. It focuses specifically on changes to statutory warrant rules and, in particular, to Rule 41. The goal is to envision how Rule 41 and equivalent state rules might be changed to respond to the specific issues raised by the switch from physical evidence to digital evidence.

Before beginning, it may be helpful to understand why this section focuses on statutory warrant rules rather than the Fourth Amendment. The primary reason is that Fourth Amendment warrant rules are far more flexible than statutory commands. As the Supreme Court has stressed,

> the Fourth Amendment's commands, like all constitutional requirements, are practical and not abstract. If the teachings of the Court's cases are to be followed and the constitutional policy served, affidavits for search warrants, such as the one involved here, must be tested and interpreted by magistrates and courts in a commonsense and realistic fashion. They are normally drafted by nonlawyers in the midst and haste of a criminal investigation. Technical requirements of elaborate specificity once exacted under common law pleadings have no proper place in this area. A grudging or negative attitude by reviewing courts toward warrants will tend to discourage police officers from submitting their evidence to a judicial officer before acting. [116]

Courts generally have heeded this guidance on the case of computer searches and seizures. For the most part, judges have proved sensitive to the practical difficulties inherent in computer searches and seizures, and they have not imposed highly restrictive requirements that would not work for the two-step warrant process.[117] Given the presumption that searches pursuant to warrants are constitutionally reasonable, courts have generally approved two-stage searches within the reasonableness framework of the Fourth Amendment.

---

[116] United States v. Ventresca, 380 U.S. 102, 108 (1965).

[117] *See supra* notes 27-64 and accompanying text.

Statutory warrant rules are less flexible and more detailed, and therefore play a greater role in light of changing facts. Statutory warrant rules such as Rule 41 are designed to regulate the traditional physical search process. They are poorly equipped to fit the two-stage search warrant process needed in the case of most computer searches and seizures. The rules remain rigid and specific, and are therefore less able to accommodate the dynamics of digital evidence searches. As a result, legal reform must focus on statutory warrant rules. Of course, constitutional and statutory rules have a symbiotic relationship. A revision of existing statutory warrant rules can help address the Fourth Amendment's reasonableness command. New statutory rules that better regulate the warrant process can permit a better fit between the new facts and the animating concerns of Fourth Amendment law.

### *A. The Thing to be Seized*

The first change I propose is modifying Rule 41's current requirement that "[t]he warrant must identify the person or property to be searched, [and] identify any person or property to be seized."[118] In digital evidence cases, more specific language should be used. The language should require the police to state what physical evidence they plan to seize on-site, and then indicate what kind of evidence they plan to search for in the subsequent electronic search. In other words, agents should be required to describe the property to be seized at *both* the physical search stage *and* the electronic search stage.

This could be achieved by amending Rule 41(e) to add an additional sentence. Something like this should work:

> If the the warrant authorizes the seizure of computers or electronic storage devices to retrieve computer data constituting evidence of crime, the warrant must identify both the

---

[118] FED R. CRIM. P. 41(e)(2).

> physical computers or storage devices to be seized and the computer data that constitutes evidence of the crime.

Under this approach, a computer warrant would require the officers to name the specific evidence they are searching for twice, correlating with the two stages of criminal investigations. For example, the warrant form could authorize the police to seize "all computers and electronic storage devices believed to contain evidence of wire fraud" while on-site and then authorize a subsequent search for the specific files that the agents have reason to believe are located on the storage device. This approach would address both the particularity concern and also ensure that the warrant is not executed in disregard of the warrant.

A second and related change should be made to Rule 41(b) and (d) to make clear that searches to retrieve information but not seize physical property are permissible. The current text of Rule 41 states that a warrant can be issued "to search for and seize a person or property located within the district."[119] When computer information is copied, however, no seizure occurs; the owner is not actually deprived of his property.[120] It is well-settled that Rule 41 can be used to obtain a warrant for mere information; this was the apparent holding of *United States v. New York Telephone Co.*,[121] and was reaffirmed in early cases holding that a Rule 41 warrant could be obtained to collect computer data.[122] However, this interpretation was reached through the meaning of "property" in Rule 41,[123] apparently without recognition that copying data does not seize it. In light of the meaning of seizure in the context of electronic evidence, it may be appropriate to modify Rule 41 formally to note that a seizure is not a prerequisite of a search.

---

[119] *Id.* at 41(b)(1).

[120] *See* Kerr, *supra* note 3, at 301.

[121] 434 U.S. 159, 170 (1977).

[122] *See, e.g.,* United States v. Hall, 583 F. Supp. 717, 718-19 (E.D. Va. 1984).

[123] *See* United States v. N.Y. Tel., 434 U.S. 159, 170 (1977).

### *B. The Place to be Searched*

Statutory warrant rules could also be amended to consider the case of computers in government custody. Alternatively, courts could simply approve warrants that describe the place to be searched in such cases as the computer itself. For example, imagine an FBI field office has a computer in its possession and needs a search warrant to search the machine. The "place to be searched" could be a particular description of the computer itself, held in the custody of the FBI field office. That is, the warrant would name the specific movable property to be searched, rather than the physical place where that movable property happens to be stored.

### *C. When Can the Search be Executed?*

Significant changes should be made to Rule 41 and equivalent state provisions to specify when each stage of the two-step warrant process must be executed. Rule 41(e)(2) states that a federal search warrant "must command the officer to: (A) execute the warrant within a specified time no longer than 10 days; (B) execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time."[124] One obvious change would be to amend this language to clarify that the ten-day and daytime rules do not apply to the subsequent electronic search, as the *Hernandez* court concluded.[125] Perhaps the easiest way to do this would be to include a definition of "execute the warrant" in the case of computer searches. For example, the following addition to the definition section of the Rule 41(a)(2) could do the trick:

> In a case involving the seizure of computers and other electronic storage devices, the execution of the warrant refers to the seizing of the computers and storage devices rather than any subsequent search of their contents.

Rule 41 also should be amended to add clear guidance on when a computer must be searched and when it should be returned. Instead of leaving this to individual magistrate judges, a uniform standard should be used. The standard should consider two important practical points. First, backlogs and delays at government forensic laboratories are common, and they are almost always beyond the control of the individual agent or prosecutor who obtains the warrant. While we might hope that the relevant legislature funds such labs properly and they can be staffed competently, it would be inappropriate to punish agents if the forensic experts have a backlog and cannot search equipment quickly. Second, when a computer device is seized only for the evidence it contains, and is not itself contraband, a fruit, or an instrumentality of crime, the government's interest in the property can be satisfied by generating a bitstream copy of the storage device. It is relatively quick and easy for a government forensic analyst to generate a bitstream copy of the storage device. Indeed, it is a necessary first step of every forensic analysis: a computer normally is searched by generating a copy of its data, and then searching the copy instead of the original.[126] In cases where the computer is used only as a storage device, the computer itself can be returned after the government has generated the bitstream copy.

---

[124] FED. R. CRIM. P. 41(e)(2).

[125] *Hernandez*, 183 F. Supp. 2d at 480-81.

In light of these practical concerns, my proposal would be to create two distinct rules to govern the timing of the forensic process. In cases where the computer is merely a storage device for evidence, the government should be required to seize the computer, create a bitstream copy of its files, and then return the property to its proper owner in a reasonable period of time, such as thirty days. The agents should be allowed to request an extension of this time period for additional thirty-day periods for good cause; this may be necessary because some computers may prove difficult to image. In addition, the rule could include provisos about ensuring that copies are recognzied to be equivalent to the original. For example, one option would be to give the defendant access to the copy and conditioning return of the computer on the defendant's stipulation that the copy is accurate. I am not sure such a provision is necessary, as investigators need to establish the reliability of computer copies in any event. At the same time, such a provision could ensure that the need to return property to a suspect does not fuel defense challenges to the accuracy of the government's copy that would be avoided in cases where the government can keep the original computer hardware.[127]

---

[126] *See* Kerr, *supra* note 8.

Requiring investigators to copy the data and returning the equipment in thirty days would also address possible constitutional problems without imposing a terrible burden on investigators. *Syphers* and *Greene* suggest that retaining a target's computer hardware for an excessive period of time may eventually render the seizure unreasonable, even pursuant to a warrant.[128] A thirty-day rule could address this concern by forcing government action and return of the computer before the seizure becomes unreasonable.

When the computer hardware is believed to be a fruit, instrumentality of crime, or contraband, the warrant should contain a different set of requirements. In these cases, the key question is whether the physical computer storage device already seized *actually is* a fruit, instrumentality of crime, or contraband. Agents generally find this out by beginning the electronic search and identifying material such as child pornography or hacking evidence. If the material is discovered on the computer, then the person from whom the property was taken has no legal right to the property; it need not be returned, and in fact will likely support legal forfeiture proceedings. In light of this, Rule 41 should require investigators to begin the forensic process and establish whether the computer contains at least some of the relevant material within a particular period of time, such as sixty days.[129] If agents locate the evidence on the computer, then they do not need to return it. However, if they cannot find any evidence showing that the computer itself is a fruit, instrumentality, or contraband, then agents should be permitted to retain the copy generated during the forensic process but should be required to and return the computer equipment. This would allow investigators to continue their search for evidence if needed, but without depriving the target of his property. As with the first set of rules, agents should be permitted to apply for extensions of time for good cause.

---

[127] Susan Brenner and Barbara Frederiksen offer a somewhat similar proposal, focused on ensuring that targets have copies of seized files rather than hardware:

> When a court issues a seizure and an off-site search authorization, it should require that the officers create at least one back-up copy of the information on the seized equipment and give this back-up copy to the owner of that equipment.

Brenner & Frederiksen, *supra* note 4, at 79.

[128] *Syphers*, 296 F. Supp. 2d 50; *Greene*, 56 M.J. at 817.

The goal of these rules would be to identify some kind of middle ground that recognizes both the difficulty of the computer forensic process and the competing interests of computer owners. A warrant to seize a computer that has a small amount of incriminating evidence on it should not provide a license for the government to seize the computer indefinitely. Instead, there should be set (if ultimately flexible) standards for when agents must generate copies of files and return the hardware in cases where the physical storage device is not independently seizable. Further, similar standards should be defined for when agents must begin the forensic process and identify whether the computer is independently seizable because the computer is contraband, a fruit, or an instrumentality of crime.

### *D. What are the Oversight and Record-keeping Requirements, and When Must Property be Returned?*

The final issue concerns oversight and record-keeping requirements, as well as the law governing when property should be returned. I think the latter question is best addressed by the rule just discussed on the timing of the forensic process. If the police are generally required to conduct enough of the forensic process at an early enough stage that the computer hardware must either be returned or the status of the property as contraband confirmed, then there is no need for a new rule specifically governing the return of property.

---

[129] *Cf.* Brenner & Frederiksen, *supra* note 4, at 84.

The question of what record-keeping requirements to mandate is difficult to answer at this time because the underlying Fourth Amendment rules remain unclear. As I detail in another article, courts have not settled on a uniform standard for reviewing the computer forensic process.[130] The record-keeping requirements of Rule 41 and analogous state rules should track the developing Fourth Amendment standards; extensive records should be kept if courts closely scrutinize the forensic process under the Fourth Amendment, but not otherwise. Until we know more about what Fourth Amendment standards apply, it is too early to settle on the proper Rule 41 standard.

One rule that does not need to be changed concerns the inventory requirement presently for the return of the warrant. The inventory requirement is presently limited to physical hardware, and in my view it should remain so limited. Susan Brenner and Barbara Frederiksen have taken a different view. They argue that the return on the warrant should include "a detailed inventory of the hardware that is seized and of the data and files that are seized."[131] They write:

> These inventories should be supplied in addition to the back-up copies of any seized data. The inventories are not substitutes for back-up copies. . . . For computer media or seized files the inventory should describe the type of media, capacity (if known), number seized, and a listing of the files contained on the media. This listing of files should detail, at a minimum, the file name, creation date, access date, file size, and the location of the file on the disk (either the full path of the file, or its absolute address on the disk).[132]

I find this approach problematic. The inventory requirement is designed to facilitate judicial review of the warrant process.[133] The suspect needs to know what was taken if he wishes to challenge the seizure. Accessing computer storage devices and compiling a list of each device's contents does not serve this function. The owner of the computer knows what is on the storage device, and taking the physical device obviously takes all of its contents. Further, such an inventory requirement may have the perverse effect of expanding the government's power to search the computer. Completing the inventory would enable the government to find out all the file names and sizes of the material on the hard drive, which might then provide clues to unrelated crimes. While such steps may or may not be acceptable under the Fourth Amendment, requiring them to be taken as part of Rule 41 allows the inventory task to serve an investigatory function.[134] On balance, I think that an inventory limited to physical storage devices should be sufficient.

---

[130] *See* Kerr, *supra* note 8.

[131] Brenner & Frederiksen, *supra* note 4, at 80.

[132] *Id.*

[133] *See generally* South Dakota v. Opperman, 428 U.S. 364, 369-71 (1976).

## CONCLUSION

Law enforcement's increasing need to collect digital evidence raises many challenges for the law of criminal procedure. The shift from physical evidence to digital evidence often leads to a shift in how investigators collect evidence; changes in how evidence is collected leads to pressure for new legal rules to regulate evidence collection. The warrant process is merely one part of a broader mosaic of the mechanisms of the investigative process that will be reformed. It is also a particularly clear example of how technology will require changes in law: computer technologies bifurcate the warrant process from its traditional one-step process to a two-step process, creating a need for legal rules to regulate the second step.

Reforming the warrant process also presents an unusual opportunity for the legal system to experiment with new legal rules in response to the shift to digital evidence. At the federal level, an advisory committee has the power to propose changes to the Federal Rules of Criminal Procedure.[135] In the case of

---

[134] United States v. Flores, 122 F. Supp. 2d 491, 494-95 (S.D.N.Y. 2000); United States v. O'Razvi, 1998 WL 405048, at *6-7 (S.D.N.Y. July 17, 1998).

[135] *See* 28 U.S.C. §§ 2072-74 (2000). Under federal law, an advisory committee created by the Judicial Conference makes recommendations to the Supreme Court,

Rule 41, the Rules Committee rather than the courts are best suited to address the problem; Rule 41 issues may occupy the time of judges and prosecutors, but they only rarely lead to litigation that can result in judicial rethinking of the legal standards.[136] The Federal Rules Committee should take the lead in this area and rethink Rule 41 for the era of digital evidence. Changes in Rule 41 can influence similar changes at the state level, and even provide an international standard that will guide other countries facing the same clash between new technologies and existing legal rules.

---

which then approves or rejects changes pursuant to a Congressional notice provision.

[136] This is true for two reasons. First, a judge's refusal to sign a warrant application is not ordinarily an appealable final order. *See* United States v. Savides, 658 F. Supp. 1399, 1404 (N.D. Ill. 1987), *aff'd in relevant part sub nom.*; United States v. Pace, 898 F.2d 1218, 1230 (7th Cir. 1990). Second, violations of Rule 41 rarely lead to suppression of evidence. *See generally* United States v. Calandra, 414 U.S. 338, 341-42 (1974).

# APPENDIX

## Federal Rules of Criminal Procedure 41.
## Rule 41. Search and Seizure

**(a) Scope and Definitions.**

**(1) Scope.** This rule does not modify any statute regulating search or seizure, or the issuance and execution of a search warrant in special circumstances.

**(2) Definitions.** The following definitions apply under this rule:

**(A)** "Property" includes documents, books, papers, any other tangible objects, and information.

**(B)** "Daytime" means the hours between 6:00 a.m. and 10:00 p.m. according to local time.

**(C)** "Federal law enforcement officer" means a government agent (other than an attorney for the government) who is engaged in enforcing the criminal laws and is within any category of officers authorized by the Attorney General to request a search warrant.

**(b) Authority to Issue a Warrant.** At the request of a federal law enforcement officer or an attorney for the government:

**(1)** a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located within the district;

**(2)** a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed; and

**(3)** a magistrate judge—in an investigation of domestic terrorism or international terrorism (as defined in 18 U.S.C. § 2331)—having authority in any district in which activities related to the terrorism may have occurred, may issue a warrant for a person or property within or outside that district.

**(c) Persons or Property Subject to Search or Seizure.** A warrant may be issued for any of the following:

**(1)** evidence of a crime;

**(2)** contraband, fruits of crime, or other items illegally possessed;

**(3)** property designed for use, intended for use, or used in committing a crime; or

**(4)** a person to be arrested or a person who is unlawfully restrained.

**(d) Obtaining a Warrant.**

**(1) Probable Cause.** After receiving an affidavit or other information, a magistrate judge or a judge of a state court of record must issue the warrant if there is probable cause to search for and seize a person or property under Rule 41(c).

**(2) Requesting a Warrant in the Presence of a Judge.**

**(A)** Warrant on an Affidavit. When a federal law enforcement officer or an attorney for the government presents an affidavit in support of a warrant, the judge may require the affiant to appear personally and may examine under oath the affiant and any witness the affiant produces.

**(B) Warrant on Sworn Testimony.** The judge may wholly or partially dispense with a written affidavit and base a warrant on sworn testimony if doing so is reasonable under the circumstances.

**(C) Recording Testimony.** Testimony taken in support of a warrant must be recorded by a court reporter or by a suitable recording device, and the judge must file the transcript or recording with the clerk, along with any affidavit.

**(3) Requesting a Warrant by Telephonic or Other Means.**

**(A) In General.** A magistrate judge may issue a warrant based on information communicated by telephone or other appropriate means, including facsimile transmission.

**(B) Recording Testimony.** Upon learning that an applicant is requesting a warrant, a magistrate judge must:

**(i)** place under oath the applicant and any person on whose testimony the application is based; and

**(ii)** make a verbatim record of the conversation with a suitable recording device, if available, or by a court reporter, or in writing.

**(C) Certifying Testimony.** The magistrate judge must have any recording or court reporter's notes transcribed, certify the transcription's accuracy, and file a copy of the record and the transcription with the clerk. Any written verbatim record must be signed by the magistrate judge and filed with the clerk.

**(D) Suppression Limited.** Absent a finding of bad faith, evidence obtained from a warrant issued under Rule 41(d)(3)(A) is not subject to suppression on the ground that issuing the warrant in that manner was unreasonable under the circumstances.

**(e) Issuing the Warrant.**

**(1) In General.** The magistrate judge or a judge of a state court of record must issue the warrant to an officer authorized to execute it.

**(2) Contents of the Warrant.** The warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

**(A)** execute the warrant within a specified time no longer than 10 days;

**(B)** execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time; and

**(C)** return the warrant to the magistrate judge designated in the warrant.

**(3) Warrant by Telephonic or Other Means.** If a magistrate judge decides to proceed under Rule 41(d)(3)(A), the following additional procedures apply:

**(A) Preparing a Proposed Duplicate Original Warrant.** The applicant must prepare a "proposed duplicate original warrant" and must read or otherwise transmit the contents of that document verbatim to the magistrate judge.

**(B) Preparing an Original Warrant.** The magistrate judge must enter the contents of the proposed duplicate original warrant into an original warrant.

**(C) Modifications.** The magistrate judge may direct the applicant to modify the proposed duplicate original warrant. In that case, the judge must also modify the original warrant.

**(D) Signing the Original Warrant and the Duplicate Original Warrant.** Upon determining to issue the warrant, the magistrate judge must immediately sign the original warrant, enter on its face the exact time it is issued, and direct the applicant to sign the judge's name on the duplicate original warrant.

**(f) Executing and Returning the Warrant.**

**(1) Noting the Time.** The officer executing the warrant must enter on its face the exact date and time it is executed.

**(2) Inventory.** An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. The officer must do so in the presence of another officer and the person from whom, or from whose premises, the property was taken. If either one is not present, the officer must prepare and verify the inventory in the presence of at least one other credible person.

**(3) Receipt.** The officer executing the warrant must:

**(A)** give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken; or

**(B)** leave a copy of the warrant and receipt at the place where the officer took the property.

**(4) Return.** The officer executing the warrant must promptly return it—together with a copy of the inventory—to the magistrate judge designated on the warrant. The judge must, on request, give a copy of the inventory to the person from whom, or from whose premises, the property was taken and to the applicant for the warrant.

**(g) Motion to Return Property.** A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.

**(h) Motion to Suppress.** A defendant may move to suppress evidence in the court where the trial will occur, as Rule 12 provides.

**(i) Forwarding Papers to the Clerk.** The magistrate judge to whom the warrant is returned must attach to the warrant a copy of the return, of the inventory, and of all other related papers and must deliver them to the clerk in the district where the property was seized.

# TRANSACTION SURVEILLANCE BY THE GOVERNMENT

*Christopher Slobogin*[*]

Many important aspects of our lives are inscribed in written and digitized records, housed in private businesses, government agencies and other institutions. These records include all sorts of information about us: reports on our medical status and financial condition; data about our purchases, rentals, real estate holdings, licenses, and memberships; logs listing the destination of our emails and our Internet wanderings; and countless other bits of individual descriptors, ranging from salary levels to college grades to driver's license numbers. Whether the information memorializes our own version of personal activities or is created by the record-holder itself, there is often an explicit or implicit understanding that the information will be used or viewed by a limited number of people for circumscribed purposes. In other words, we consider the contents of many of these records private, vis-a-vis most of the world.

Thus, it may be surprising that law enforcement officials can, perfectly legally, gain access to all of this information much more easily than they can search our houses or even our cars. While the latter types of actions require probable cause, government can obtain many of the records just described simply by asking (or paying) for them.[1] And, at most, all the government needs to show in order get any of these records is that they are "relevant" to a government investigation–a much lower, and much more diffuse, level of justification than probable cause.[2]

---

[*] Stephen C. O'Connell Professor of Law, University of Florida Fredric G. Levin College of Law. For their comments on this paper, I would like to thank Jerold Israel, Scott Sundby, Peter Swire, George Thomas, and participants in workshops or symposia at the following schools: Mississippi, DePaul, Florida State, Ohio State, and Hastings.

[1] *See generally* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137 (2002).

This state of affairs might make sense when the records sought are truly public in nature. It might also be justifiable when the records involve an entity such as a corporation, professional service provider, or government department and are sought in an effort to investigate the entity and its members. But today, facilitated by the computerization of information and communication, government routinely obtains *personal* medical, financial and email records, in connection with investigations that have nothing to do with business or governmental corruption.[3] That practice is much more questionable.

This article explores the scope and regulation of what I will call "transaction surveillance" by the government. That term is meant to distinguish the subject of this article from both "physical surveillance" and "communications surveillance." Physical surveillance is real-time observation of physical activities, using either the naked eye or enhancement devices such as binoculars or video cameras. Communications surveillance is real-time interception of the content of communications, relying on wiretapping, bugging, hacking, and various other methods of intercepting oral statements and wire and electronic transmissions. Transaction surveillance, in contrast, involves accessing *already-existing* records, either physically or through computer databanks. It also encompasses accessing, in real-time or otherwise, the *identifying signals* of a transaction (such as the address of an email recipient).[4]

Like physical and communications surveillance, transaction surveillance is a potent way of discovering and making inferences about a person's activities, character and identity. Yet, despite a bewildering array of statutorily created authorization requirements, transaction surveillance by the government is subject to far less regulation than either physical surveillance of activities inside the home or communications surveillance.[5] My principal argument is that transaction surveillance should be subject to much more legal monitoring than it is.

---

[2] *See infra* text accompanying notes 35-37.

[3] *See* Solove, *supra* note 1.

[4] This tripartite division of surveillance was developed by the American Bar Association's Task Force on Law Enforcement and Technology and is explicated further in Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards*, 10 HARV. J. L. & TECH. 383, 387-88 (1997).

To get to that conclusion, this article proceeds in four parts. Part I explains why government, and in particular law enforcement, finds transaction surveillance so attractive, and why it is so easy to carry out in this digital age. Part II describes the current law regulating transaction surveillance. Not only is this regulation minimal, it is confusing and contradictory; beyond the traditional subpoena, challengeable by the target of the investigation, current law recognizes a number of subpoena mutations that seem to have little rhyme or reason. If it contributes nothing else, this article should at least clarify the nature of today's regulatory framework.

Part III criticizes this framework and outlines a more promising approach. The proposed reform recognizes, as does the current regime, that different sorts of records merit different levels of protection. But, in contrast to current law, the proposal would significantly increase the degree of protection in a number of situations, to the probable cause level for personal records held by private and public entities and to the reasonable suspicion level for personal records readily available to the public.

Part IV concludes by examining alternatives to the proposal (and to the current regime). It rejects both an approach that requires probable cause for all records searches and, at the other extreme, an approach that would allow suspicionless records searches on condition that anything discovered is subject to strict limitations on disclosure. It also criticizes an approach that relies on the legislature, rather than the courts and the Fourth Amendment, to establish fundamental regulatory requirements. Not all recorded information warrants the maximum refuge from government intrusion. But much of it deserves much more protection than it receives today.

---

[5] As discussed *infra* text accompanying notes 38-82, transaction surveillance never requires probable cause. In contrast, communications surveillance requires a warrant,, which may be issued only if there is probable cause and other methods of obtaining the information have failed. *See* 18 U.S.C. § 2518(3). Physical surveillance of the home requires a warrant unless it can take place with the naked eye from a lawful vantage point using technology that only replicates such naked eye viewing or it involves technology that is in general public use. Kyllo v. United States, 533 U.S. 27, 34-35 (2001).

## I. THE CURRENT REACH OF TRANSACTION SURVEILLANCE

Transaction surveillance comes in many forms. This article divides it into two types: target-based and event-based. Using these categorizations, the following discussion relies on hypotheticals to flesh out the various ways transaction surveillance can assist law enforcement in investigating street crime.

### A. *Target-Based Transaction Surveillance*

Assume that I'm a federal agent, and that I'm suspicious of you for some vague reason–perhaps you often pay for your airplane tickets with cash,[6] or you have been observed with accessories you shouldn't be able to afford,[7] or you are a young, Arab male who goes to the local mosque on a daily basis.[8] Under these types of circumstances, I clearly do not have sufficient suspicion for an arrest.[9] On the other hand, I feel I would be neglecting my obligation as a law enforcement official if I did not investigate you a bit further. So how do I find out more about you?

---

[6] *Cf.* Florida v. Royer, 460 U.S. 491, 493 n.2 (1983) (noting that paying for an airline ticket with cash is often an element of drug courier profiles used by the Drug Enforcement Administration).

[7] *Cf.* State v. Cookson, 361 S.W.2d 683, 684 (Mo. 1962) (informant, who alleged that defendants had robbed a tavern, reported that "they had a large sum of money and were spending freely").

[8] *Cf.* Michael J. Whidden, *Unequal Justice: Arabs in America and United States Antiterrorism Legislation*, 69 FORDHAM L. REV. 2825, 2865 (2001) (recounting FBI surveillance of a Brooklyn mosque).

[9] An arrest or prolonged questioning in the stationhouse requires probable cause. CHARLES H. WHITEBREAD & CHRISTOPHER SLOBOGIN, CRIMINAL PROCEDURE:

I could confront you directly, either on the street or through a grand jury.[10] But neither approach is likely to net much information, and both will tip you off that I'm checking you out. Ditto with respect to going to your acquaintances and neighbors; they will probably not be complely forthcoming and they might let you know I've been nosing around. I could try the undercover agent approach–there might be rich payoffs if I or one of my informants can weasel into your good graces. But success at that endeavor is rare, and spending so much effort on someone about whom I'm merely suspicious would usually be a waste of time. I could also surreptitiously follow you around for awhile, but that tactic is unlikely to produce much, especially if you make most of your contacts through technological means–phones, email–rather than physical travel. Of course, I could tap your phone and intercept your emails, but that requires a warrant based on probable cause, which I do not have.

Thankfully there are other, much more efficient ways I can covertly acquire information about you, many of which I can carry out without leaving my desk and most of which, as the next section describes, require no or little legal authorization. The easiest way to get useful data is to contact one of the many companies, usually called commercial data brokers (CDBs), that use computers and the Internet to dig up "dirt" from public and not-so public records.[11] One such company is LexisNexis, the legal research bohemoth, which operates

---

AN ANALYSIS OF CASES AND CONCEPTS 72-76 (4th ed. 2000).

[10] Note further that even questioning in the field that lasts longer than a few minutes requires reasonable suspicion, which exists only if there are specific and articulable facts that the person is or has been engaging in criminal activity. *Id.*

[11] In fact, the website for one of these companies can be found at "digdirt.com". The services are of uneven quality. *See* Preston Gralia, *Digital Gumshoes*, *available at* http://www.pcmag.com/article2/0,4149,20148,00.asp (Nov. 13, 2001) (recounting efforts to use various services, including digdirt, with mixed results). For present purposes, however, the point is that their potential for transaction surveillance is enormous.

Accurint, a program that allows "organizations to quickly and easily extract valuable knowledge from . . . tens of billions of data records on individuals and businesses," armed with no more than a name, address, phone number, or social security number.[12] Through this process, I can obtain information about a wide array of your transactions, including: bankruptcies and corporate filings, criminal convictions and criminal and civil court data (including marriage and divorce information), driver's licenses and motor vehicle information, firearms, hunting, fishing and professional licenses and permits, Internet domain names, property deeds and assessments, and voter registration information.[13] For some states, the information held in "public records" by government bureaucracies and available via computer is immensely broader: some types of medical records, Social Security numbers, crime victim's names, credit card and account numbers, psychiatric evaluation reports, tax returns, payroll information, and family profiles.[14] For a time, all of this was made even more easily accessible to state law enforcement officials through MATRIX (Multi-State Anti-Terrorist Information Exchange), a multistate consortium that allowed police to use Accurint for investigative purposes until its federal funding was discontinued in 2005.[15]

The FBI and other federal agencies rely on equally powerful commercial data brokers, with perhaps the most popular being Choicepoint.[16] Under its contract with the federal government, Choicepoint can provide me, as a federal agent, with "credit headers" (information at the top of a credit report which includes name, address, previous address, phone number, social security number and employer); pre-employment screening information (including financial reports, education verification, reference verification, felony check, motor vehicle record and professional credential verification); "asset location services"; information about neighbors and family members; licenses (driver's, pilot's and professional); business information compiled by state bureaucracies; and "derogatory information" such as arrests, liens, judgments and bankruptcies.[17] If you think I wouldn't bother requesting such a check, think again; between 1999 and 2001, Choicepoint and similar services ran between 14,000 and 40,000 searches per month for the United States Marshall's Service *alone.*[18]

---

[12] *See* Accurint Website, *available at* www.accurint.com/aoutus.html (last accessed on Sept. 13, 2005). LexisNexis bought Accurint from SeisInt in 2005.

[13] *Id.*

[14] Robert Ellis Smith, *Here's Why People Are Mad*, 29 PRIVACY J. 7, 7 (Jan. 2003) (citing Stephen Grimes, administrator of the Judicial Records Center in Rhode Island), *available at* http://www.privacyjournal.net/.

[15] *See* Fla. Dep't Law Enforcement, MATRIX Pilot Project Concludes (April 14, 2005), *available at* http://www.fdle.state.fl.us.press_releases/20050415_matrix_project (noting, however, that Florida and several other states may continue funding the program).

[16] *See* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L & COMM. REG. 595, 617-18 (describing the FBI's "secret, classified contract" with Choicepoint).

The one drawback to the type of information I get from CDBs is that it is pretty general. I may want to know more about what you do on a daily basis. Fortunately, there are a number of services that can help me out. For instance, advances in data warehousing and data exchange technology in the financial sector allow very easy access to a virtual cornucopia of transaction-related information that can reveal, among other things, "what products or services you buy; what charities, political causes, or religious organizations you contribute to; . . . where, with whom, and when you travel; how you spend your leisure time; . . . whether you have unusual or dangerous hobbies; and even whether you participate in certain felonious activities."[19] If I jump through some pro forma legal hoops (detailed in Part II), I can also get records of all the phone numbers you dial and receive calls from,[20] and from your Internet Service Provider (ISP) I can get every website address you have visited (so-called "clickstream data") and every email address you have contacted.[21]

---

[17] *Id.* at 601-02. Note also that once a social security number and other identifying information is obtained, other personal informaticn might become much more easily accessible. *See* Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89, 108-14 (2001) (pointing out that schools, financial institutions and other entities make personal information accessible by anyone with the right Social Security number, address, and mother's maiden name).

[18] *Id.* at 4-6. In 2001, the Immigration and Naturalization Service conducted approximately 23,000 such searches a month. *Id.* at 11.

[19] Janet Dean Gertz, *The Purloined Personality: Consumer Profiling in Financial Services*, 39 SAN DIEGO L. REV. 943, 944-45, 951 (2002).

The latter information can be particularly revealing to the extent you transact your business over the Internet. Recently some ISPs, like America OnLine, have stopped maintaining clickstream data, precisely so they won't have to answer such law enforcement requests.[22] No worries. All I have to do is invest in something called "snoopware." Bearing names like BackOrifice, Spyagent, and WinWhatWhere,[23] snoopware is to be distinguished from adware and spyware. The latter software tells the buyer of the program how to contact people who visit the buyer's website. Snoopware, in contrast, allows its buyer to track the target well beyond a single website; it accumulates the addresses of *all* the Internet locations the target visits, as well as the recipients of the target's emails. The FBI has developed a similar program, once dubbed Carnivore, now called DCS-1000, that filters all emails that pass through a particular server.[24] Although some transaction snoopware requires access to the server or computer to install, other types, called Trojan Horses, can electronically worm their way onto the system disguised as something useful.[25]

---

[20] The Electronic Communications Privacy Act, 18 U.S.C. § 3121 allows prosecutors to obtain this information by certifying to a court that it is "relevant" to an ongoing investigation. *See infra* text accompanying notes 43-47.

[21] The Electronic Communications Privacy Act at most requires a showing of relevance for this information. *See* 18 U.S.C. § 3121; *infra* notes 69-77 and accompanying text; *see also* Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. J. TELECOMM. & TECH. L. REV. 61, 68-69 (2000) (detailing the type of information government can obtain through clickstream data).

[22] Conversation with Peter Swire, Professor, Ohio State School of Law, September 20, 2004. The Electronic Frontier Foundations has recommended that ISPs only keep personally identifiable communications logs for "so long as it is operationally necessary, and in no event for more than a few weeks." Electronic Frontier Foundation, *Best Data Practices for Online Service Providers*, from the Electronic Frontier Foundation *at* http://www.eff.org/osp/20040819_OSPBestPractices.pdf2 (June 29, 2005).

[23] *See* Cade Metz, *Spyware: It's Lurking on Your Machine*, PC MAG., Apr. 22, 2003, at 85, 88.

[24] Jeremy C. Smith, *The USA PATRIOT Act: Violating Reasonable Expectations of Privacy Protected by the Fourth Amendment Without Advancing National Secu-*

In short, even if you stay at home and conduct all your business and social life via phone, email and surfing the 'Net, I can construct what one commentator has called "a complete mosaic" of your characteristics.[26] And I can do all of this without you having a clue I'm doing it. It is also possible that I could surreptitiously obtain an even wider array of transactional information–on matters ranging from medical treatment to financial decisions–with very little effort. But further discussion of that possibility, as well as of the huge amount of transactional information that government can obtain if it is willing to proceed overtly, will have to await Part II's explanation of the current legal regime.

### *B. Event-Based Transaction Surveillance*

Now consider an entirely different type of scenario, one in which government has no suspicion of or even interest in a specific individual, but rather possesses information about a particular crime that has been or will be committed. Government efforts to obtain transactional data in this situation is not target-based, but event-based. Say, for instance, that the police know that a sniper-killer wears a particular type of shoe (thanks to mudprints near a sniper site), that he owns a

---

*rity*, 82 N.C. L. REV. 412, 448-49 (2003). Recently, the FBI announced that it would no longer use DCS-1000, but instead rely on "unspecified commercial software to eavesdrop on computer traffic." *FBI Cuts Carnivore Internet Probe*, *at* http://www.cnn.com/2005/TECH/internet/01/18/fbi.carnivore.ap/index.html (on file with the *Mississippi Law Journal*).

[25] Metz, *supra* note 23, at 85. Some snoopware, using "key logger" technology, can even tell the user the content of one's computer screen. *Id.* DCS-1000 can also be programmed to access content as well as identifying information. Joseph F. Kampherstein, *Internet Privacy Legislation and the Carnivore System*, 19 TEMP. ENVTL. L. & TECH. J. 155, 167 (2001). Both functions are forms of communications surveillance that are beyond the scope of this article.

[26] Anthony Paul Miller, *Teleinformatics, Transborder Data Flows and the Emerging Struggle for Information: An Introduction to the Arrival of the New Information Age*, 20 COLUM. J. L. & SOC. PROBS. 89, 111 (1986).

particular type of sweater (because of threads found at another site), and that he reads Elmore Leonard novels (because of allusions to those books made in his communications to the police). Law enforcement understandably might want to peruse the purchase records of local shoe, clothing, and book stores as part of their investigation. Once police obtain the credit card numbers of those who bought, say, the type of sweater found at the murder scene, they can trace other purchases made with the same card, to see if the relevant type of shoe or book was bought by any of the same people. Of course, if there is a match on two or three of the items, the surveillance may then turn into a target-based investigation.

Or say that a CIA informant reports that he believes Al Qaeda is considering blowing up a major shopping mall, using skydivers jumping from rental planes.[27] The FBI might want to requisition the records of all companies near major metropolitan areas that teach ski-diving and that rent airplanes, as well as the "cookie" logs (records of cyberspace visitors) of all websites that provide information about manufacturing explosives, to see if there are any intersections between these three categories of data, in particular involving men with Arab-sounding names. If there are then, again, further target-based surveillance investigation might take place.

Although the first type of event-based surveillance is backward-looking and the second is forward-looking, both law enforcement efforts are a form of what has been called "data mining" or "profiling," that is, an attempt to look through transaction information to find patterns of behavior that permit police to zero in on possible suspects.[28] If the information sought is not digitized, which is likely with respect to records kept by ski-diving companies, for instance, then law enforcement may have to rely on good old-fashioned human snooping. In this day and age, however, a significant amount of data mining can be carried out using technology. For example, the Defense Department's Total Information Awareness program, before it was severely limited by Congress, would have used software developed by private companies "to sift through virtual mountains of data of everyday transactions, such as credit card purchases, e-mail and travel itineraries, in an attempt to discover patterns predictive of terrorist activity."[29] Whether it relies on computers or humans, event-based data mining, like transaction surveillance of particular individuals, can easily be conducted unbeknownst to those whose records are surveilled.

---

[27] This imaginary scenario is borrowed from the second Markle Report. Markle Foundation, Creating a Trusted Network for Homeland Security: Second Report of the Markle Foundation Task Force, app. D at 121-33 (2003), *available at* http://www.markletaskforce.org/.

[28] For a general description of data mining and its prevalence, see Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 71-88 (2003).

### *C. Summary*

Technology has made transaction surveillance a particularly powerful law enforcement tool. Given the potential that transaction surveillance provides the government for creating personality mosaics and linking people to crime, it could well be even more useful than visual tracking of person's activities (physical surveillance) and eavesdropping on or hacking into a person's communications (communications surveillance). But the real beauty of transaction surveillance for the government is that, compared to physical surveillance of activities inside the home and communications surveillance, it is so lightly regulated. As Part II explains, under today's regulatory regime it is much easier for government to obtain information about our most intimate transactions, including medical and financial matters, than it is to intercept our communications about those transactions.

## II. CURRENT LEGAL REGULATION OF TRANSACTION SURVEILLANCE

Under the Fourth Amendment, the government usually cannot conduct a search of houses, persons, papers and effects without probable cause,[30] a relatively high level of certainty akin to a more-likely-than-not standard (which, in non-exigent situations, must be found by a magistrate pursuant to an application for a warrant).[31] For some less invasive actions (a frisk, for instance), police only need reasonable suspicion, which is a lower level of certainty than probable cause but still requires "specific and articulable facts" that "criminal activity may be afoot," to quote from the famous case of *Terry v. Ohio*.[32] Finally, in some "special needs" situations (searches of school children or employees; drug testing; health and safety inspections; roadblocks), the police need only act "reasonably," but that test still usually requires reasonable suspicion,[33] or at least a showing that those conducting the government action are pursuing some end other than criminal law enforcement.[34]

---

[29] *Id.* at 64; *see also infra* note 122.

In contrast, transaction surveillance, whether it is event-based or target-based, *never* requires probable cause or reasonable suspicion, even when conducted by government agents whose primary goal is criminal investigation. At most, government agents seeking transactional information need a subpoena–either a subpoena duces tecum issued by a grand jury, or an "administrative subpoena" issued by a government agency–which is valid as long as the information it seeks is "relevant" to a legitimate (statutorily-authorized) investigation. Relevance, as defined by the Supreme Court, is an extremely low standard. In the grand jury context, a subpoena may be quashed on irrelevancy grounds only when the court "determines that there is no reasonable *possibility* that the *category* of materials the Government seeks will produce information relevant to the *general subject* of the grand jury's investigation."[35] The relevancy standard in the administrative subpoena context is even lower, with the Supreme Court holding that "[e]ven if one were to regard the [subpoena] as caused by nothing more than official curiosity, nevertheless law-enforcing agencies have a legitimate right to satisfy themselves that corporate behavior is consistent with the law and the public interest."[36] In short, the link between the information a subpoena commands and the investigation the government is pursuing can be very tenuous indeed. Although a subpoena may be challenged before it is executed, a successful challenge is exceedingly rare, whether the subpoena is issued by a grand jury or an administrative agency.[37]

---

[30] *See* U.S. CONST. amend. IV.

[31] *See* WHITEBREAD & SLOBOGIN, *supra* note 9, at 137-42.

[32] 392 U.S. 1, 21, 30 (1968).

[33] *See* O'Connor v. Ortega, 480 U.S. 709, 724 (1987) ("The delay in correcting the employee misconduct caused by the need for probable cause rather than reasonable suspicion will be translated into tangible and often irreparable damage to the agency's work, and ultimately to the public interest."); New Jersey v. T.L.O., 469 U.S. 325, 341-42, 344 (1985) (holding that "a search of a student by a teacher or other school official will be 'justified at its inception' when there are reasonable grounds for suspecting that the search will turn up evidence" and finding that this standard was met in this case because there was reasonable suspicion).

[34] *See* Bd. of Educ. v. Earls, 536 U.S. 822, 829 (2002) (upholding warrantless, suspicionless school drug testing, noting that "in the context of safety and administrative regulations, a search unsupported by probable cause may be reasonable when 'special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable'"); City of Indianapolis v. Edmond, 531 U.S. 32, 41 (2000) ("We have never approved a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing. Rather, our checkpoint cases have recognized only limited exceptions to the general rule that a seizure must be accompanied by some measure of individualized suspicion.").

Furthermore, as we shall see, the law does not require even a traditional subpoena for most types of transaction surveillance. Instead, the government, in particular Congress, has either invented new forms of authorization that are even easier to obtain or has simply permitted unrestrained law enforcement access to transactional information. The following account of this incredibly weak regulatory regime starts with the law regarding transaction surveillance of identifying information, conducted in real-time, then describes regulation of government attempts to obtain public records, and finally describes transaction surveillance of records held by private entities.

---

[35] United States v. R. Enters., Inc., 498 U.S. 292, 301 (1991) (emphasis added).

[36] United States v. Morton Salt Co., 338 U.S. 632, 652 (1950); *see also* United States v. Powell, 397 U.S. 48, 57-58 (1964) (holding that administrative subpoenas are valid if the records sought are "relevant" to an investigation conducted for a "legitimate purpose"); United States v. Hunton & Williams, 952 F. Supp. 843, 854 (D.D.C. 1997) (holding that the *Powell* inquiry is more deferential than the "arbitrary and capricious" standard of review for agency action under the Administrative Procedure Act).

[37] *See* WAYNE R. LAFAVE, JEROLD H. ISRAEL & NANCY J. KING, 3 CRIMINAL PROCEDURE 134 (2d ed. 1999) ("Courts generally give grand juries considerable leeway in judging relevancy."); JACOB A. STEIN, GLENN A. MITCHELL & BASIL J. MEZINES, 3 ADMINISTRATIVE LAW 20-59 (2002) ("[S]ubpoenas will be enforced as to any documents that 'are not plainly immaterial or irrelevant to the investigation.'").

### A. *Interception of Transaction Information*

Real-time government interception of the *content* of communications (what I am calling communications surveillance) is prohibited unless authorized by a warrant based on probable cause.[38] In contrast, interception of the identifying features of the communication–the names of the communicators, their phone numbers or email addresses, and the addresses of websites visited–can take place on a much lesser showing. The Fourth Amendment does not apply at all to this type of transaction surveillance, and statutory law places virtually no restrictions on it.

The Fourth Amendment's justification requirements–probable cause and the like–only apply if government engages in a "search or seizure." Although one might reasonably label government efforts to track down a person's phone and email correspondents a search, the Supreme Court has held that a *Fourth Amendment* search occurs only when a government action infringes a reasonable expectation of privacy.[39] More importantly for present purposes, the Court has determined, in *Smith v. Maryland*,[40] that we do not have a reasonable expectation in the phone numbers we dial because we know or should know that phone companies keep a record of these numbers, and thus "assume the risk" that the phone company will decide to disclose this information to the government.[41] Because it is generally known that Internet service providers monitor, if only temporarily, our emails and Internet surfing, the Court would probably also say that we assume the risk these providers will become government informants. Although Universal Resource Locators (URLs) can be more informative than a mere phone number, both because they are addresses (e.g., www.amazon.com/kidneydisease) and because they allow access to the website and thus permit government to ascertain what the user has viewed, the lower courts applying *Smith* appear to see no difference between the two types of routing information.[42] Accordingly, the government can probably ignore the Fourth Amendment when intercepting phone numbers *and* Internet addresses.

---

[38] 18 U.S.C. § 2518(3). The court must also find that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." *Id.* § 2518(3)(c).

[39] Kyllo v. United States, 533 U.S. 27, 33 (2001) ("[A] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.") (citing Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

[40] 442 U.S. 735 (1979).

---

[41] *Id.* at 744 ("[P]etitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business . . . [thereby] assum[ing] the risk that the company would reveal to police the numbers he dialed.")

[42] *Cf.* Thygeson v. U.S. Bancroft, No. CU-03-467-ST 2004 WL 2066746 (D. Or. Sept. 15, 2004) ("[W]hen the information defendants collected was only the website addresses, rather than the actual content of the websites Thygeson visited, [the surveillance] is analogous to a pen registry search, where in the Fourth Amendment context, courts have held that defendants have no reasonable expectation of privacy in the telephone numbers they dial because the numbers are conveyed to the telephone company."); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) ("When defendant entered into an agreement with Road Runner for Internet service, he knowingly revealed all information connected to the IP address . . . ."); *see also infra* note 46. Billing records of ISPs may also be unprotected by the Fourth Amendment. United States v. Hambrick, 225 F.3d 656 (4th Cir. 2000) (unpublished opinion) (holding that person does not have a reasonable expectation of privacy "in the account information given to the ISP in order to establish the e-mail account, [because it] is non-content information" disclosure of which "to a third party destroys the privacy expectation that might have existed previously"), *available at* 2000 U.S. App. LEXIS 18665, at *12. Indeed, some courts have held that the *content* of email messages, once they are opened, deserve no Fourth Amendment protection because one assumes the risk the recipient will reveal it to others. United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997); Smyth v. Pillsbury, 914 F. Supp. 97, 101 (E.D. Pa. 1996); United States v. Maxwell, 45 M.J. 406, 417-18 (C.A.A.F. 1996).

Congress has imposed some statutory restraints on this type of surveillance, but nothing approaching the usual Fourth Amendment protections. In the Electronic Communications Privacy Act of 1986 (ECPA), it created a new, streamlined type of authorization process for use of pen registers (technology which intercepts outgoing phone numbers) and trap and trace devices (technology which intercepts incoming numbers), a process that can be initiated by either a federal government attorney or a state law enforcement officer. All the government agent must do is certify to a court facts that show the information is "relevant to an ongoing investigation" and is "likely to be obtained by [the surveillance]."[43] If that certification is made, the court *must* issue the order.[44]

The USA Patriot Act of 2001 expanded the definition of pen registers and trap and trace devices to include all devices that obtain "dialing, routing, addressing, or signaling information utilized in the processing and transmitting of wire or electronic communications . . . "[45] Thus, to use snoopware, DCS-1000, and other means of ascertaining a person's email correspondents and favorite websites, the government need only certify the relevance of this information to a current investigation.[46] Again, if this certification is made, the court must issue an order.

Those of us who teach Fourth Amendment law sometimes joke about supposedly "neutral and detached" magistrates rubberstamping warrant applications, but we also assume that judicial independence is theoretically possible.[47] Here, in contrast, Congress has legislatively invented *mandatory* rubberstamping. It is tempting to call this type of authorization a "rubberstamp order," but I will instead use the more measured term *certification order*. Whatever one calls the authorization process, it amounts to minimal limitation on interception of transaction information.

---

[43] 18 U.S.C. § 3123(a)(1) (2000).

[44] United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995) (the "judicial role in approving use of trap and trace devices is ministerial in nature").

[45] 18 U.S.C. § 3121(c) (2000).

[46] Most courts have held that companies that acquire "clickstream data" about where an Internet user goes on the Internet do not violate ECPA because the websites visited by the user have authorized the companies to access this information. *See In re* DoubleClick, Inc., Privacy Litig., 154 F. Supp. 2d 497, 526 (S.D.N.Y. 2001); Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1163 (W.D. Wash. 2001); *In re* Toys R Us, Inc., Privacy Litig., No. C00-2746 2001 U.S. Dist. LEXIS 16947, at *28 (N.D. Cal. Oct. 9, 2001). Thus, government could also obtain routing information from these private companies, without using snoopware. However, some courts might consider that approach to be accessing "stored" information. *See, e.g.*, United States v. Steiger, 318 F.3d 1039, 1050 (11th Cir. 2003). If so, government may have to obtain a subpoena. *See infra* text accompanying notes 65-68.

### *B. Access to Publicly-held Records*

Most transaction surveillance does not involve real-time interception of information, but rather contemplates accessing already-existing records, held either by public or private institutions. Information in public records is particularly easy to secure. Under current law, law enforcement officials do not need even a certification order to use MATRIX, Choicepoint and similar vehicles for perusing public records. In fact, law enforcement officials need consult *no* other entity (certainly not a court, and not even a prosecutor) before obtaining such information.

Again, the Fourth Amendment's ban on unreasonable searches and seizures might appear to apply here, because looking for and through records is a search in the usual meaning of the word. But, as already noted, the Supreme Court has made clear that one cannot reasonably expect privacy in connection with information voluntarily given to third parties. Even more important than *Smith* in this regard is *United States v. Miller*,[48] decided three year earlier. There the Court held that once a person surrenders information to an agency or institution, he or she assumes the risk the third party will hand it over to the government.[49] The key declaration in *Miller* is worth quoting in full: "[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, *even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed*."[50]

---

[47] See RICHARD VAN DUIZEND, L. PAUL SUTTON & CHARLOTTE A. CARTER, THE SEARCH WARRANT PROCESS: PRECONCEPTIONS, PERCEPTIONS AND PRACTICES 47-48 (1985) (describing study of warrant process indicating varying degrees of judicial rubberstamping across jurisdictions).

[48] 425 U.S. 435 (1976).

The Privacy Act, enacted by Congress in 1974, does bar or limit access to public records when they are sought by private individuals, and even when most government officials want them.[51] But when *law enforcement* officials are after the records, the Act merely requires a letter from the head of the agency that is seeking the information, detailing the law enforcement reasons a particular person's records are needed.[52] No court is involved, and neither individualized suspicion or even a relevance showing is required, just the sayso of the law enforcement department. I will call this kind of authorization an *extrajudicial certification*.

Not even this level of authorization is necessary for government access to most public records, however. The Privacy Act only applies to federal documents. Unless there is similar legislation at the state level, law enforcement access to state public records is unrestricted.[53] Furthermore, the federal government takes the position that when it obtains information from a commercial data broker like Choicepoint, the Privacy Act does not apply at all, because the Act literally only refers to law enforcement efforts to get records from other government agencies and from private companies that are administering a system of records for the government.[54] Under this interpretation, the only obstacle to complete government access to all the data maintained by commercial brokers is the price of the information.[55]

---

[49] *Miller*, 425 U.S. at 443.

[50] *Id.* at 443 (emphasis added).

[51] *See* 5 U.S.C. § 552a(b) (2000) ("No agency shall disclose any record which is contained in a system of records . . . unless [listing 12 exceptions].").

[52] *Id.* § 552a(b)(7) (permitting disclosure "to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought").

[53] *See* Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 605 (1995) (most states lack "omnibus data protection laws," but rather have "scattered laws [that] provide only limited protections for personal information in the public sector."). One reason Florida is an attractive place to base an operation like MATRIX is that its public records law is quite extensive. *See* FLA. STAT. § 119.01 *et seq.* ("It is the policy of this state that all state, county and municipal records

### *C. Access to Privately-held Records*

Compared to the meager limitations on intercepting transactional information and accessing public records, the restrictions on government access to the contents of records held by nominally private entities, such as hospitals and banks, phone companies and Internet providers, have more teeth, but the teeth are blunt. Again, the Fourth Amendment is pretty much irrelevant here. The notion that one assumes the risk that third parties will be, or turn into, government informants applies to private entities as well as public agencies. The Supreme Court has specifically so held with respect to phone companies (in *Smith*)[56] and banks (in *Miller*).[57] It has wavered in its willingness to declare private entities untrustworthy confidants only in the medical context, where it has stated, in dictum, that the Fourth Amendment or the due process clause *might* place constitutional limitations on law enforcement access.[58] Although there are also statutory constraints

---

shall be open for personal inspection by any person."). Recognizing this problem, the Florida Supreme Court recently ordered a moratorium on the digitization of Florida's public records. Jason Krause, *Too Much Information? County Clerks Tussle with Nervous State Officials Over Posting Court Records Online*, A.B.A. J., April 2004, at 24.

[54] 5 U.S.C. § 552a(m).

[55] *See* Hoofnagle, *supra* note 16, at 623 ("[A] database of information that originates at a CDB would not trigger the requirements of the Privacy Act [, thus allowing CDBs] to amass huge databases that the government is legally prohibited from creating.").

[56] *Smith*, 442 U.S. at 744.

[57] *Miller*, 425 U.S. at 443.

[58] *Cf.* Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001) ("The reasonable

on government accessing of privately-held records, they are extremely weak.

Medical records receive the most protection. Even here, however, neither probable cause or reasonable suspicion is required. Rather, pursuant to rules promulgated under the Health Insurance Portability and Accountability Act (HIPAA), the government can obtain medical records from HMOs and hospitals with a simple subpoena. A subpoena, it will be recalled, merely requires a finding that the information sought is relevant to a law enforcement investigation (although the target is entitled to notice and thus has the opportunity to challenge the subpoena on relevance or privilege grounds).[59] Given the limited scope of the Privacy Act described above, even that obstacle is removed if, as is true in some states, medical and similar information is maintained as a "public record" and the government receives it through a commercial data broker.

Financial records receive similarly minimal protection. To get detailed information from credit agencies, a regular subpoena is required under the Fair Credit Reporting Act.[60]

---

expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent."); Jaffee v. Redmond, 518 U.S. 1, 15 (1996) ("Because we agree with the judgment of the state legislatures and the Advisory Committee that a psychotherapist-patient privilege will serve a public good transcending the normally predominant principle of utilizing all rational means for ascertaining truth, . . . we hold that confidential communications between a licensed psychotherapist and her patients in the course of diagnosis or treatment are protected from compelled disclosure under Rule 501 of the Federal Rules of Evidence."); Whalen v. Roe, 429 U.S. 589, 605 (1977) (recognizing, in the context of a case involving disclosure of medical information, that a "statutory or regulatory duty to avoid unwarranted disclosures . . . in some circumstances . . . arguably has its roots in the Constitution").

[59] 45 C.F.R. § 164.512(f)(1)(ii)(B) (2005) (disclosure of medical records under HIPAA is permissible without permission of their subject if information is sought for law enforcement purposes through a grand jury subpoena). Some courts have required a greater showing to obtain medical records. *See, e.g.,* Doe v. Broderick, 225 F.3d 440, 450-51 (4th Cir. 2000) (finding *Miller* inapplicable to medical records); Haw. Psychiatric Soc., Dist. Branch of American Psychiatric Ass'n v. Ariyoshi, 481 F. Supp. 1028 (D. Haw. 1979); King v. State, 535 S.E.2d 432, 495 (Ga. 2000); Thurman v. State, 861 S.W.2d 96, 98 (Tex. Ct. App. 1993).

[60] 15 U.S.C. § 1681b(a)(1). Name, addresses, and places of employment can be

However, analogous to the situation with medical records, no law governs government requests for similar information from database companies and other companies that have obtained it from credit agencies.[61] As a result, the government routinely gets the financial information it wants directly from a commercial data broker, without bothering with a subpoena.[62] Bank records are also easily accessible. The Right to Financial Privacy Act generally requires only a traditional subpoena to obtain financial records from a bank. It also recognizes a significant variation to the traditional subpoena process: notification of the seizure may be delayed for up to 90 days if there is concern that service of the subpoena will tip off a suspect, result in loss of evidence, endanger witnesses or in some other way compromise the government's investigation.[63] In these circumstances, in contrast to the typical subpoena process, the target of a financial investigation will not find out that the government has the information until well *after* it is obtained. I will call this type of authorization a *delayed-notice subpoena*.

Outside of situations covered by the Right to Financial Privacy Act and the Internal Revenue Code, a government agency that is authorized to use administrative subpoenas to obtain financial and business information from third party entities need not give *any* notice to the customer whose records are sought.[64] This practice recognizes still another sub-

---

obtained simply upon a request. *Id.* § 1681f.

[61] Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1146 (2002).

[62] Chris Hoofnagle has made the argument that this ability to obtain information through a private agency circumvents the Privacy Act, which prohibits government from collecting such information unless there is a specific need for it. Hoofnagle, *supra* note 16, at 18.

[63] 12 U.S.C. § 3409. Furthermore, when subpoena power is not available to the government, it need only submit a formal written request for the information, a process this article calls extrajudicial certification. § 3408. Indeed, apparently banks sometimes still simply hand over information upon request. *See* DAVID F. LINOWES, PRIVACY IN AMERICA: IS YOUR PRIVATE LIFE IN THE PUBLIC EYE? 106-108 (1989) (describing a number of cases in which banks surrendered account information to law enforcement officers simply upon request and describing a survey finding that seventy-four percent of banks did not inform their customers of their routine disclosures to law enforcement).

[64] ELLEN S. PODGOR & JERRY H. ISRAEL, WHITE COLLAR CRIME IN A NUT-

poena mutation, which I will call an *ex parte subpoena*. This label is meant to distinguish between third party subpoenas that allow the target to contest the demand for production and those that don't. The term "ex parte subpoena" emphasizes that the customer is outside the process entirely, thus removing, in most cases, the only meaningful inhibition on fishing expedition-by-subpoena.

Transaction surveillance of communications-related information is regulated in a similarly weak fashion. Under ECPA, real-time interception of the content of phone and email communications requires a warrant based on probable cause.[65] But if email has sat on a server for longer than 180 days without being opened, or the recipient of email or voicemail accesses it and stores it on an outside server for any length of time, then a subpoena–delayed if necessary–is all that is needed to obtain the content of the communication.[66] Apparently, the rationale behind permitting easy access to unopened mail that is stored for 180 days is that it is, in effect, abandoned.[67] The rationale for permitting access on less than probable cause to opened email and other communications stored by a third party is that it becomes akin to a business record.[68]

---

SHELL 269 (2004).

[65] 18 U.S.C. § 2518(3) (2000).

[66] 18 U.S.C. § 2703(a) (2000); 2703(b)(1)(B). Further, a subpoena is only required when the information is sought from a "remote computer service" (e.g., a service available to the general public, like AOL). If the information is stored with a service not available to the general public (e.g., one run by an employer), then ECPA does not apply *at all* and government may obtain the stored information (content or identifying) simply upon a request. *See* 18 U.S.C. § 2703(a)(1-3); *see also* 18 U.S.C. § 2711(2) (2000) (defining remote computing service); U.S. Dep't of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 89 (July 2002), *available at* http://www.cybercrime.gov/s&smanual2002.htm.

[67] *See* Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1421 (2004). This article is an extremely helpful roadmap and analysis of ECPA which, unfortunately, I discovered only after wading through the statute myself. *Id.*

[68] *See* CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING § 26:9 (2d ed. 1995) (explaining that Congress felt that when an e-mail stays on a server longer than 180 days the service provider is less like a Post Office and more like a storage facility).

ECPA also gives the government easy access to business records held by phone companies and Internet service providers. Under Title II of ECPA, as amended by the Patriot Act of 2001, basic subscriber information–name, address, session times and durations, length and type of service, means and source of payment (including credit card numbers), and the identity of Internet users who use a pseudonym–can be obtained pursuant to an ex parte subpoena, the type of authorization that requires no customer notice.[69] If the government seeks additional transactional information–such as account logs and email addresses of other individuals with whom the account holder has corresponded–it still need not alert the subscriber, but must allege "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation."[70]

Apparently, this latter standard, found in § 2703(d) of ECPA, is meant to be more demanding than the relevance standard normally required for a subpoena. Yet it is not clear that it is much different. Although the "specific and articulable" language sounds like it requires reasonable suspicion, note that the specific and articulable facts need only support a finding that the information is *relevant* and *material* to an ongoing investigation. Even if the latter highlighted word is meant to augment the former, it does not add much; materiality, in evidence law, merely means that the evidence be logically related to a proposition in the case.[71] Furthermore, whereas *Terry* contemplated that reasonable suspicion exist with respect to the targeted individual, a § 2703(d) order, like a subpoena, allows accessing *any* records that might be relevant to an investigation, not just the target's. Finally, it is not clear that the "relevant and material" language can be meaningfully enforced. The statute seems to say that the only ground on which an order issued pursuant to § 2703(d) may be challenged is burdensomeness, which eliminates a challenge on relevance grounds.[72]

---

[69] 18 U.S.C. § 2703(c)(1)(E) (2001) (describing information that can be obtained); § 2703(c)(3) ("A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.").

[70] § 2703(c) (describing requirements for a court order to obtain "[r]ecords concerning electronic communication service or remote computing service").

[71] McCormick on Evidence § 185 at 276-78 (John W. Strong ed., 5th ed. 1999) ("Materiality . . . looks to the relation between the propositions that the evidence is offered . . . and the issues in the case. . . . A fact that is 'of consequence' is material . . . . It is enough if the item could reasonably show that a fact is slightly more probable than it would appear without that evidence.").

Post-9/11, government access to some sorts of privately-held records is even easier when a significant purpose of the investigation is to nab terrorists or spies. In such cases, Section 215 of the Patriot Act authorizes the FBI to demand the production of "any tangible things (including books, records, papers, documents and other items)" if it follows a simple two-step process.[73] First, the Director or his or her designee must certify to a court that the items sought are "for an investigation to protect against international terrorism or clandestine intelligence activities," and that the investigation does not focus "solely" on activities protected by the First Amendment.[74] Second, the court must find that the investigation meets these conditions; if so, it "shall" issue a Section 215 order authorizing the seizure.[75] In other words, a variant of the certification order discussed in connection with use of pen registers and trap and trace devices will suffice in this situation. In an additional twist, however, not only is the target unable to challenge such orders, but the third party record-holder is *prohibited* from telling the target the order has been issued.[76] In counter-terrorist investigations, this procedure is all that is required to obtain customer records of Internet service providers, libraries, video stores, schools and other private entities (including, possibly, medical providers). Further, the records that may be obtained in this way are not just those of suspected terrorists, but those of anyone who might be "relevant" to the investigation.[77]

---

[72] § 2703(d) (providing court may quash or modify order if the request is "unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider").

[73] 50 U.S.C. § 1861 (2001).

[74] § 1861(a) & (b).

[75] § 1861(c). This provision also indicates that the judge may modify the government's order. Apparently, the modification power is meant to protect against First Amendment and overbreadth concerns. But, assuming no such concerns, the judge must issue the order when the tangible items sought are "for an authorized investigation . . . to obtain foreign intelligence information." § 1861(b). *Cf.* Paul Rosenzweig, *Civil Liberty and the Response to Terrorism*, 42 DUQ. L. REV. 663, 694-95 (2004) (arguing that the provision for judicial modification, together with the requirements that the government swear the certification is correct and that the Attorney General report to Congress on the use of Section 215, provide more safeguards than those associated with a subpoena reviewable only after challenge).

Finally, even a Section 215 order is not needed when the FBI is seeking a particular subset of "tangible items" (electronic or communication records, financial records or credit records) in connection with a national security investigation. Rather, all it must do is issue a form of administrative subpoena, known as a "National Security Letter," in which a Special Agent (in other words, a field agent) certifies that the information sought is relevant to a national security investigation to protect against international terrorism or clandestine intelligence activities.[78] This type of authorization is akin to the extrajudicial certification discussed in connection with law enforcement efforts to seek public documents under the Privacy Act, but with the same gag order proviso that exists with Section 215 orders.[79]

The Patriot Act allowed this extrajudicial process with respect to financial information only when it was held by banks. However, in December, 2003, that power was expanded by the Intelligence Authorization Act of 2003, which was enacted by Congress as part of an appropriations bill, with no vetting by the Judiciary Committee and no debate on the floor or in the media.[80] The 2003 Act allows the FBI to use extra-judicial certification to obtain statements and records from *any* financial institution "whose cash transactions have a high degree of usefulness in criminal, tax or regulatory matters," including banks, stockbrokers, car dealers, casinos, credit card companies, insurance agencies, jewelers, pawn brokers, travel agents and airlines.[81] All of this information is the government's simply on its sayso.[82]

---

[76] 18 U.S.C. § 2709(c) (2001); 50 U.S.C. § 1861(d).

[77] Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1331-33 (2004); *see also* 18 U.S.C. § 2709(b) (wire or electronic service providers); 20 U.S.C. § 1232g(j)(A) (school records); Kathryn Martin, *The USA Patriot Act's Application to Library Patrons Records*, 29 J. LEGIS. 283 (2003) (discussing library records).

[78] 12 U.S.C. § 3414(a)(5)(A) (2003). Again, the record-holder is prohibited from informing the target of the request. § 3414(a)(5)(D).

[79] Swire, *supra* 77, at 1332-33.

### *D. Summary of Transaction Surveillance Law*

Transaction surveillance has spawned a wide array of new regulatory schemes, which are usefully summarized by locating them within the standard Fourth Amendment hierarchy. As noted earlier, the most protective type of authorization is the warrant, based on probable cause. Although intercepting the content of communications and physical surveillance of the home both require a warrant,[83] no type of transaction surveillance requires this most demanding form of authorization. The next type of authorization in the hierarchy, at least in theory, is an order based on reasonable suspicion, or what could be called a *Terry* order, after *Terry v. Ohio*,[84] which required this degree of justification for a stop and frisk. Again, none of the statutory provisions I have described (or any other regulatory regime for that matter) mandates this type of order; I include it both for the sake of comprehensiveness and because it is important to the regulatory scheme I propose below. After a *Terry* order comes the traditional subpoena, issued upon a judicial finding of relevance and challengeable by the target. This is the first type of authorization that plays a role in transaction surveillance; subpoenas are required to access most medical, financial and stored email records.

---

[80] Kyle O'Dowd, *Congress Hands FBI "Patriot II" Snooping Power*, 28 Feb. CHAMP. 18 (2004)

[81] 31 U.S.C. § 5312 (1996).

[82] The Patriot Act's National Security Letter (NSL) provision was declared unconstitutional in *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (2004), because of the lack of judicial review and the gag provision. However, the decision did not find fault with either the relevance standard or the fact that letters can be issued by a special agent. Indeed, the court stated "the standard of review for administrative subpoenas similar to NSLs is so minimal that most such NSLs would likely be upheld in court." *Id.* at 502. Recent proposed amendments at most are likely to codify *Doe*. Eric Lichtblau, *Congress Nears Deal to Renew Antiterror Law*, N.Y. TIMES, Nov. 17, 2005, at A1, A21. In the meantime, the FBI issues roughly 30,000 NSLs a year, maintains all the records thereby obtained (even when not linked to terrorism), and as of this writing had still not responded to a year-old congressional request for information about their use. Barton Gellman, *The FBI's Secret Scrutiny*, WASH. POST (Nov. 6, 2005), at A1.

[83] *See supra* note 5.

Below the traditional subpoena is the delayed-notice subpoena, which authorizes, temporarily, unobstructed access to financial records and stored email when a traditional subpoena might frustrate the investigation. Next is the ex parte subpoena (unchallengeable by the target), which allows access to many types of customer records held by third party entities, including phone and ISP account records.[85] The certification (judicial rubberstamp) order follows in the hierarchy; it authorizes the use of pen registers, trap and trace devices and other forms of transaction-oriented snoopware, as well as tangible items other than financial records thought to be relevant to national security investigations.[86] At the bottom of the authorization totem pole there is the extrajudicial certification, which permits access to public records, and to financial and other records relevant to national security investigations. However, even this type of authorization is not needed to access public records that come from a state with no privacy statute or that are accumulated by a commercial data broker. All of the authorization mechanisms described in this paragraph are statutory inventions, and are particularly punchless given the lack of a remedy in the unlikely event government is found to have abused them.[87]

---

[84] 392 U.S. 1 (1968).

[85] Arguably, the "specific and articulable facts" ex parte subpoena required by 18 U.S.C. § 2703(d) is more difficult to obtain than an ordinary subpoena (and apparently Congress so believed), but for the reasons suggested above, *see supra* notes 69-72 and accompanying text, it is classified here as less protective than a regular subpoena, at least one that notifies the target.

[86] People who have worked at the Department of Justice state that, in practice, a certification order may be harder to obtain than a subpoena. Personal conversations with Orin Kerr (Feb. 17, 2005) and Paul Ohm (Jan. 20, 2005). But I rank the certification order lower in the hierarchy of protection because the judge plays such a minimal role; at least with a subpoena the judge is permitted to find a seizure invalid on relevance grounds, although he may rarely do so.

The chart below depicts the foregoing summary, consisting of eight levels of authorization:

CURRENT LAW OF TRANSACTION SURVEILLANCE

| Transaction | Auth'zation Req'd | Certainty Level |
|---|---|---|
| ——— | Warrant | Probable cause |
| ——— | *Terry* Order | Reasonable suspicion |
| Medical, financial & tax records; stored email | Subpoena | Relevance, challengeable by target |
| Financial records and stored email if notification poses risks | Delayed-notice Subpoena | Relevance, challengeable by target only after records obtained |
| Billing records and logs of phone companies & ISPs; most customer records | Ex Parte Subpoena | Relevance, challengeable only by third party record-holder |
| Interception of catalogic information re calls & email; tangible items re terrorism | Certification Order | Relevance (determined by government), issued by court, challengeable only by third party record-holder |

---

[87] For instance, there is no exclusionary sanction under ECPA, or under the Right to Financial Privacy Act. WHITEBREAD & SLOBOGIN, *supra* note 9, at 344-45; United States v. Kington, 801 F.2d 733, 734 (5th Cir. 1986). Nor are damages actions a significant deterrent, given the intangible nature of the harm involved. *Cf.* Doe v. Chao, 306 F.3d 170, 177 (4th Cir. 2002) (holding that, under ECPA, "a person must sustain actual damages to be entitled to the statutory minimum damages award" of $1,000).

| | | |
|---|---|---|
| Federal public records; financial records re terrorism | Extrajudicial Certification | Relevance (determined by government), not challengeable by any party(?)[88] |
| State public records not protected by law or that are acquired by a CDB | None | None |

## III. A Proposal for Regulation of Transaction Surveillance

The differences between the various types of authorization outlined above are sometimes subtle, but one thing is certain: their number goes well beyond (and below) the traditional three-tiered approach of probable cause, reasonable suspicion, and special needs/reasonableness determinations, all challengeable by the target of the investigation. As a conceptual matter, a system that recognizes more than three authorization levels may make sense. In previous work, for instance, I have argued for application of a proportionality principle, which specifically requires that the certainty required for a search be roughly proportionate to its intrusiveness, and which suggests that the traditional probable cause/reasonable suspicion dichotomy is insufficient as a means of implementing that idea.[89] My disagreement with current law is not with the general approach, but with the order and substance of the hierarchy.

The degree to which transaction surveillance is regulated should not depend on whether the information sought is intercepted in real-time or is stored, or on whether it may be related to terrorist actions or some other crime. Rather, the key variables should be the type of information sought and the type of transaction surveillance (target-based or event-based) that is at issue. I propose recognizing three types of distinctions based on the type of records sought: (1) the content of personal records would be entitled to more protection than the content of organizational records; (2) the content of personal records held by private entities would be entitled to more protection than the content of personal records held by public entities for public consumption; and (3) the content of records, regardless of their subject or who holds them, would presumptively be entitled to more protection than records memorializing what I call "catalogic data" (information that simply identifies the nature of a communication or links a person to an activity). With catalogic data, however, the second variable mentioned above–the government's motivation in carrying out the surveillance–is also important. If the information is sought in connection with target-based, as opposed to event-based, surveillance it should receive heightened protection.

---

[88] *See supra* note 82 and accompanying text.

[89] Christopher Slobogin, *Let's Not Bury* Terry*: A Call for Rejuvenation of the Proportionality Principle*, 72 ST. JOHN'S L. REV. 1053, 1081-82 (1998); Christopher Slobogin, *The World Without A Fourth Amendment*, 39 UCLA L. REV. 1, 68-75 (1991).

More specifically, I propose that government should have to obtain: (1) a warrant based on probable cause when it seeks the content of personal records, or seeks catalogic data in connection with target-based surveillance; (2) a *Terry* order based on reasonable suspicion when it seeks the content of records that are "public" in nature; (3) a traditional subpoena based on relevance–or when there is concern about tipping off a suspect, a delayed-notice subpoena based on relevance[90]–to access the content of organizational records and to access catalogic data in connection with event-based transaction surveillance. Ex parte subpoenas, certification orders and extrajudicial certifications should *never* be sufficient authority to carry out nonconsensual searches and seizures for personal transaction information, except in emergencies, and then only if quickly subject to judicial review. The following chart represents my proposal:

---

[90] Orin Kerr notes that, given the ease with which subpoena-service delays can be obtained, the government can use subpoenas "without meaningful notice." Orin S. Kerr, Symposium, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1234 (2004). He also argues that the ninety-day delay period "serves no legitimate purpose," and instead proposes a thirty-day delay, permitted only upon judicial authorization, with (rare) further extensions only after further judicial review. *Id.* at 1235. This regime seems sensible.

PROPOSED LAW OF TRANSACTION SURVEILLANCE

| Transaction | Auth'zation Req'd | Certainty Level |
|---|---|---|
| Content of privately-held personal records | Warrant | Probable Cause |
| Content of publicly-held personal records | *Terry* Order | Reasonable Suspicion |
| Content of organizational records | Subpoena | Relevance |
| Catalogic Data |  |  |
| Target-based surveillance | Warrant | Probable Cause |
| Event-based surveillance | Subpoena | Relevance |

Under this scheme, again, the contents of "personal" records are distinguished from the contents of "impersonal," organizational records, with acquisition of the former requiring something more than mere relevance. Within the "personal" record category, "privately-held" records are distinguished from "publicly-held" records, with acquisition of the former requiring probable cause and of the latter reasonable suspicion. Finally, "content" is distinguished from "catalogic data" that simply describes the nature of a transaction, with the authorization level for the latter dependent on whether it is sought in connection with event-based surveillance of the type involved in data mining and profiling, where only relevance is required, or target-based surveillance which requires probable cause. The reasoning behind these proposals, and definitions of the key terms, follow, beginning with the all-important distinction between organizational and personal transactions.

### A. *Organizational v. Personal Content*

In a previous article, *Subpoenas and Privacy*, I canvassed several possible justifications for the current relaxed state of transaction surveillance regulation.[91] Although I discussed six such justifications, they all fit within one of two categories: they either minimize privacy concerns associated with transactional information or rest on an assertion that law enforcement could not function if transaction surveillance were subject to significant regulation. I also concluded that these rationales are not unpersuasive in the context in which subpoenas first flourished–government efforts to obtain documentary evidence of crimes committed by or within a business or other regulated organization. As the Supreme Court has recognized on numerous occasions, records of businesses and similar entities are associated with a minimal degree of privacy, given their impersonal nature and the high degree of state regulation to which organizations are subject.[92] The Court has also pointed out in several cases that investigation of economic crimes and regulatory violations would be extremely difficult without ready access to documents detailing business activity.[93] But my previous analysis also concluded that neither the diminished-privacy rationale or the heightened-need justification applies when the records sought are personal.

The diminished-privacy rationale, as applied to personal records, is both descriptively and normatively flawed. When such records are retained by the individual, they are thought to be, and ought to be, as private as anything else in one's home. Even when maintained by a third party, records about an individual are, and should be, considered similarly private if, as is usually the case, the transfer or collection of the information occurred because the third party *requires* it in order to carry out an important societal service. Hospitals, banks, Internet service providers and public agencies usually only have personal data because we must provide it (or allow it to be accumulated) in order to receive the services these entities provide. Stated another way, most third party record-holders possess information about us because we cannot otherwise realistically function in the modern world. Thus, contrary to the Supreme Court's assertion in *Miller*, the surrender of personal information to these third parties is hardly "voluntary." Nor does it, or should it, lead us to "assume" that the third party will function as an institutional undercover agent, a conduit for any information the government wants.[94]

---

[91] Christopher Slobogin, *Subpoenas and Privacy*, 34 DEPAUL L. REV. 805 (2005).

[92] In *Hale v. Henkel*, 201 U.S. 43 (1906), the leading Supreme Court case on grand jury document subpoenas, the Court stated that while a corporation "is a creature of the state . . . [it] is presumed to be incorporated for the benefit of the public [and] "receives certain special privileges and franchises, and holds them subject to the laws of the state and the limitations of its charter," while an individual "owes no such duty to the state, since he receives nothing therefrom, beyond the protection of his life and property." *Id.* at 74. In *United States v. Morton Salt Co.*, 338 U.S. 632 (1950), one of the Court' leading administrative subpoena cases, it was even more forthright: "[C]orporations can claim no equality with individuals in the enjoyment of a right to privacy." *Id.* at 652.

[93] *See, e.g.,* United States v. White, 322 U.S. 694, 700 (1944) ("The scope and nature of the economic activities of incorporated and unincorporated organizations and their representatives demand that the constitutional power of the federal and state governments to regulate those activities be correspondingly effective.").

The argument that more rigorous regulation of transaction surveillance would unduly hinder the government's law enforcement efforts is also weak when applied to personal records. There is no doubt that requiring probable cause to obtain records will make investigation of crime more difficult. But to convert that fact into a rationale for removing restrictions on government evidence-gathering makes a mockery of constitutional protections, for the warrant and probable cause requirements always have that effect. In this context as well, a viable distinction exists between investigations of organizational activity and investigation of street crime and the like. Evidence of organizational crime, particularly of the economic variety, is largely if not entirely documentary; indeed, without such evidence even the victims of such crime may not realize it has occurred. But the same is seldom true of other types of crime. Whereas "it is a fact of life that agencies charged with regulating economic activity often cannot articulate probable cause or even reasonable suspicion that a violation has transpired without first examining documents reflecting a party's economic activity,"[95] police engaged in investigating other types of criminal activity usually can develop some non-documentary lead, whether it is from the victim, a third party eyewitness, or physical surveillance of public movements.[96]

---

[94] Empirical research confirms that most people view a search of records containing their personal information to be at least as intrusive as a search of a car or luggage. *See* Christopher Slobogin & Joseph Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society"*, 42 DUKE L.J. 727, 738-39 (1993) (Table 1) (finding that a sample of 217 individuals, on average, ranked "perusing bank records" as more "intrusive" than searches of the trunk of a car and a footlocker in a car); *see also* Lior Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005) (arguing that, under social networks theory, information revealed to small social groups should generally be considered private unless the target's actions or status removes it from obscurity).

If one accepts these arguments, then it is important to separate personal from organizational documents. Fortunately, as I explained in *Subpoenas and Privacy*,[97] the Supreme Court has already done much work in this regard, in the course of defining the concept of a "collective" entity and the notion of "required records" for purposes of determining when there is a Fifth Amendment right to resist documentary subpoenas. Although the Court's reconceptualization of the Fifth Amendment in the mid-1970s has rendered these cases largely irrelevant for Fifth Amendment purposes,[98] they are directly pertinent to the current task of identifying which types of records are associated with minimal privacy. That is because these cases explicitly tried to demarcate when records are entitled to what the Court eventually called "a zone of privacy."[99] In essence, in its collective entity cases the Court concluded that the records of any organization that has an identity separate from its individual members lie outside that zone.[100] In its required records cases, the Court similarly held that the government may force individuals to keep and disclose documents that are crucial for regulating their activities and "have assumed 'public aspects' which render [the records] at least analogous to public documents."[101] Consistent with these two lines of cases, records that pertain to a collective entity or that fit the required-records criteria ought to be accessible on mere issuance of a subpoena.

---

[95] Parks v. FDIC, 65 F.3d 207, *11 (1st Cir. 1995), *withdrawn* 64 USLW 2166 (Selya, J., dissenting).

[96] SARA SUN BEALE ET AL., 1 GRAND JURY LAW & PRACTICE 6-3 (2d ed. 2002) ("Ordinarily, investigations of so-called 'street crimes' such as murder, rape, robbery, and assault, can be conducted effectively without resort to the subpoena power."); KENNETH MANN, DEFENDING WHITE COLLAR CRIME: A PORTRAIT OF ATTORNEYS AT WORK 233-34 (1985) (noting that the easiest crimes to hide are those where the victim does not realize he or she has been victimized, those where the location of the crime is "not apparent"–making witnesses hard to identify–and those where the "inculpatory information is embedded in normal social life," all factors much more likely to be associated with organizational rather than individual crime).

[97] Slobogin, *supra* note 91.

[98] The crucial decision was *Fisher v. United States*, 425 U.S. 391 (1976), which decisively moved the Court's Fifth Amendment jurisprudence from a focus on privacy to a focus on coercion. There the Court held that because a document

Other records, however, should receive more protection. The Fourth Amendment specifically speaks of searches of papers, as well as searches of persons, houses, and effects, and it usually requires probable cause for these searches. Accordingly, subpoenas demanding the contents of personal records should generally be invalid under the Fourth Amendment unless they are based on such a showing. The rest of this section discusses whether there should be any other exceptions to this rule outside of the organizational investigation setting.

---

subpoena does not compel the creation of documents, it only implicates the Fifth Amendment when the act of production it compels provides the prosecution with useful incriminating information. *See also* Andresen v. Maryland, 427 U.S. 463 (1976) (holding that a search warrant compels neither the creation *or* production of documents).

[99] Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

[100] *See* Bellis v. United States, 417 U.S. 85, 92, 94-95 (1974) (holding that even though a small law firm "embodies little more than the personal legal practice of the individual partners," it is a "formal institutional arrangement organized for the continuing conduct of the firm's legal practice," and thus was "an independent entity apart from its individual members").

[101] *See* Grosso v. United States, 390 U.S. 62, 67-68 (1968) (describing the components of the required records doctrine established in *Shapiro v. United States*, 335 U.S. 1 (1948)).

### *B. Private v. Public Records*

One distinction regarding personal records that could be made is between those records that are "private" and those that are in the public domain. As the required-records line of cases suggests, when the records fit in the latter category, the privacy associated with their content is considerably diminished. With truly public records, the information can no longer be said to be "owned" solely by the individual and the recordholder. In that instance, reasonable suspicion–the justification level that falls between probable cause and relevance–ought to be sufficient justification for permitting government access.

Public records and records held by a public entity are not synonymous however. The word "public" can apply to functionally "private" institutions such as hospitals, schools and libraries, as well as to courthouses and government agencies. And even government agencies can house records that are more personal than public.[102]

How can we determine when public records are not really public and therefore deserving of full Fourth Amendment protection? Once again, statutory law and litigation in other contexts have already ploughed this ground. In particular, provisions in the federal Freedom of Information Act and similar state statutes are directly on point. While these laws establish a presumption in favor of disclosure of records held by government agencies, primarily as a means of increasing government transparency and facilitating social transactions such as business deals,[103] they usually exempt from disclosure a wide array of "personal" records. Thus, under the federal statute, government agencies must resist a FOIA request for "commercial or financial information obtained from a person and privileged or confidential,"[104] "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy,"[105] and law enforcement records to the extent they include information that "could reasonably be expected to constitute an unwarranted invasion of personal privacy."[106] State FOIA statutes or interpretive caselaw protect various other types of records. For instance, Florida, which is known as the Sunshine State not only because of its weather but also because of the breadth of its public records disclosure law, nonetheless exempts from unrestricted disclosure some types of motor vehicle registration information,[107] identifying information relating to health care provided by the state,[108] credit information held by state agencies,[109] and educational records.[110] In many states, some types of licensing information are also exempt from disclosure.[111]

---

[102] *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 127 (2002) (describing "a system where the government extracts personal information from the populace and places it in the public domain").

[103] *Id.* at 140.

[104] 5 U.S.C. 552(b)(4). Many circuits have held that voluntarily submitted infor-

---

mation will be deemed "confidential" for the purpose of this exemption if it is of a kind that would customarily not be released to the public by the person from whom it has obtained records. *See, e.g.,* Critical Mass Energy Project v. Nuclear Regulatory Comm'n, 975 F2d 871, 872 (D.C. Cir. 1992), *cert. denied*, 507 U.S. 984 (1992). *See generally What Constitutes "Trade Secrets and Commercial or Financial Information Obtained from Person and Privileged or Confidential," Exempt from Disclosure under Freedom of Information Act (5 U.S.C.A. § 552(b)(4)) (FOIA)*, 139 A.L.R. FED. 225 (2004).

[105] *Id.* § 552(b)(6). The Supreme Court has defined "similar files" broadly, to include "detailed Government records on an individual which can be identified as applying to that individual," U.S. Dep't of State v. Washington Post Co., 456 U.S. 595, 602 (1982), although it has also made clear that such files cannot be withheld simply because such identification cannot be guaranteed, and that redaction of identifying names may be sufficient. Department of Air Force v. Rose, 425 U.S. 352, 381-82 (1976). *See generally* Annotation, *When Are Government Records "Similar Files" Exempt from Disclosure under Freedom of Information Act Provision (5 U.S.C.A. § 552(b)(6)) Exempting, Certain Personnel, Medical, and "Similar" Files*, 106 A.L.R. FED. 94 (2004).

[106] *Id.* at 552(b)(7)(c). Thus, for instance, a person's rap sheet may be exempt from disclosure. See U.S. Dep't of Justice v. Reporter's Comm. for Freedom of Press, 489 U.S. 749, 774 (1989). *See generally* James O. Pearson, Annotation, *What Constitutes "Unwarranted Invasion of Personal Privacy" for Purposes of Law Enforcement Investigatory Records Exemption of Freedom of Information Act (5 U.S.C.A. sec. 552(b)(7)(C))*, 52 A.L.R. FED. 181 (2004).

[107] FLA. STAT. § 119.07(aa).

[108] *Id.* at (bb), (cc), & (hh).

[109] *Id.* at (dd).

[110] FLA. STAT. § 1002.22(d).

[111] *See, e.g.,* Mager v. State Dep't of Police, 595 N.W.2d 142, 143 (1999) (hold-

When federal or state law indicates that information found in government records should be withheld despite the strong interest in freedom of information, it ought to be considered private for Fourth Amendment purposes as well. That should mean that law enforcement must demonstrate probable cause to obtain it. For other records held by public entities, reasonable suspicion is sufficient.

Recall, however, that even this latter level of justification demands more than the current legal regime, which usually does not even require a subpoena in such situations, but rather permits law enforcement access to public records with a simple extrajudicial certification. A curious law enforcement officer should not be able to sift through the personal data found in divorce papers, real estate documents and court proceedings without articulating a specific need for it. That articulation should take place beforehand to a judge or, in the manner typical of a subpoena, after notification and challenge.[112]

A common complaint about such an approach is that it places more limits on government officials than on members of the public, who can access public records at will and, with the advent of Google and other Internet search services, can do so more easily than ever before. But most of the time the public only seeks public information when it has a specific need for it (akin to the reasonable suspicion standard).[113] More importantly, government's resources and power are so much more significant, and its hunger for information so much more voracious, especially post-9/11, that its potential for abusing per-

---

ing that "gun ownership is information of a personal nature'" requiring exemption from the state freedom of information act); *see also* OR. REV. STAT. § 656.702(1) ("[t]he records of the State Accident Insurance Fund Corporation, *excepting employer account records and claimant files*, shall be open to public inspection.") (emphasis added).

[112] Note that this procedure is no more onerous, from the law officer's perspective, than the current pen register regime. *See supra* notes 43-47 and accompanying text.

[113] Noah Rothbaum, *Spies Like Us*, SMART MONEY (Feb. 2005) at 89-92 (describing the various ways people might and do use new search engines, including investigating job applicants and real estate for sale).

sonal information far exceeds anything individuals or even corporations might do.[114]

### C. Catalogic Data

By "catalogic data" I mean information that classifies and describes a transaction, as distinguished from the content of the transaction. Catalogic data includes descriptors of communications and transmissions, such as phone numbers dialed, the addresses that route emails, and the duration of phone calls and Internet session times. This category of transactional information also includes membership lists; plane, train and ship passenger manifests; business records listing who purchased what and when; and other archives that describe the identities of those who have participated in a particular activity or communication.

This listing overlaps with some of the information that ECPA permits the government to obtain with an ex parte subpoena or a certification order. However, I would not include within the rubric of catalogic data other types of personal information ECPA currently allows government to obtain with an ex parte subpoena, such as the URLs of websites visited or the identity of those using pseudonyms.[115] This kind of information is more akin to content: the URLs can be used to visit the same websites the target visits, and disclosure of the person behind the pseudonym will often allow government to link that person to particular messages.[116]

So limited, catalogic data should not be entitled to as much protection as the content of communications, because it is not as personal as the substance of communications made during the transaction. That is not to say, as the Supreme Court has said, that the Fourth Amendment is irrelevant when something other than content is at issue. *Smith v. Maryland* notwithstanding,[117] most of us would not expect the people who work at our phone company (or Internet service provider) to care who we call (or write to), an expectation that is undoubtedly correct.[118] But the evidence that catalogic data provides about content is, at best, circumstantial. Catalogic data is to the substance of the contact as the visage is to personality. Thus, while it is entitled to some protection, catalogic data should not be treated in the same way the associated content is.

---

[114] *See infra* notes 142-46 and accompanying text (describing concerns about government's ability to obtain and abuse information); *see also* SOLOVE, *supra* note 102, at 168-75 (describing current government efforts to obtain information about millions of citizens and concluding that "we are already closer to Total Information Awareness than we might think") & 175-87 (describing possible abuses of information-gathering, including "creeping totalitarianism," inhibition of freedom of association, and J. Edgar Hoover's misuse of surveillance against alleged communist party members and people like Martin Luther King).

[115] *See supra* notes 69-72 and accompanying text.

[116] *See generally* John Alan Farmer, Note, *The Specter of Crypto-Anarchy: Regulating Anonymity—Protecting Peer-to-Peer Networks*, 72 FORDHAM L. REV. 725 (2003).

The analysis changes, however, when the government uses technologically-enhanced transaction surveillance to *aggregate* catalogic data. When information from pen registers, snoopware programs, and commercial data broker programs is combined, it can identify all of our surreptitious connections with the world, providing powerful evidence of our activities and beliefs.[119] To use the words of the commentator quoted earlier, law enforcement can construct a "complete mosaic of a person's characteristics" through this type of transaction surveillance. Under these circumstances, the information the government accumulates is more akin to content than mere cataloguing. The visage analogy no longer applies.

This distinction between aggregated and isolated catalogic data roughly maps onto the distinction between target-based and event-based transaction surveillance described earlier.

---

[117] *See supra* notes 40-41 and accompanying text.

[118] *Cf.* Wayne LaFave, *The Forgotten Motto of Obsta Principis in Fourth Amendment Jurisprudence*, 28 ARIZ. L. REV. 291, 302 (1986) (bank officials do not have "direct, significant contact with the underlying transactional information" in the same way law enforcement officers who collect all of an individual's financial information would) (quoting Note, 83 YALE L.J. 1439, 1463-64 (1974)).

[119] *See generally* Stan Karas, *Privacy, Identity, Databases*, 52 AM. U. L. REV. 393, 398 (2002) ("What we buy is how we present ourselves to the outside world; it represents how we choose to interact with it . . . . These preferences are expressive, revealing and private.").

When government has identified a target, it will tend to accumulate as much information as possible about the target. Under such circumstances, the transaction surveillance will produce a personality "mosaic" that is deserving of maximum protection.

Event-based transaction surveillance of catalogic data is usually different. Recall the example given earlier of the sniper investigation in which police find a sweater thread and footprint they believe belong to the sniper, and also know that the sniper reads a particular type of detective novel. Law enforcement attempts to identify the sniper through accessing the records of local clothing, shoe and bookstores are likely to disclose the names of numerous innocent people who have purchased items similar to those thought to be owned by the criminal. But this information, while personal, is merely a piece of the mosaic, not nearly the complete picture that target-based surveillance is likely to produce. In this situation, a relevance showing should be enough, at least when the access does not infringe First Amendment interests.[120]

However, ex parte subpoenas, certification orders and extrajudicial certifications, which are the current means of regulating access to catalogic data when there is any regulation at all, are insufficiently restrictive despite their reliance on the relevance standard. These devices leave the transaction surveillance decision about personal data entirely or almost entirely in the discretion of law enforcement even when no exigent circumstances exist, a notion that is antithetical to the Fourth Amendment.[121] Instead, in non-emergency situations

---

[120] The Supreme Court has indicated that requiring an individual engaged in advocacy to surrender anonymity without good cause can infringe First Amendment interests. *See, e.g.,* NAACP v. Alabama *ex. rel.* Patterson, 357 U.S. 449, 462 (1958) ("It is hardly a novel perception that 'compelled disclosure of affiliation with groups engaged in advocacy may constitute [an] effective . . . restraint on freedom of association.'"); Shelton v. Tucker, 364 U.S. 479, 490 (1960) (prohibiting compelling teachers to disclose group memberships).

[121] As Justice Jackson stated in *Johnson v. United States*, 333 U.S. 10, 13-14 (1948):

> The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the

the government should be able to obtain catalogic data in connection with event-based surveillance only when a judge finds it is relevant to an investigation, an assertion the record-holder should have the opportunity to challenge unless notification would undermine the investigation.

### *D. Data Mining/Profile Information*

Data mining is event-based transaction surveillance–the use of records searches to discern patterns of behavior that can be linked to past or future crime, without having a specific individual or individuals in mind. Several formal data mining programs exist. For instance, the Homeland Security Department runs something called the Electronic Surveillance System for Early Notification of Community-Based Epidemics (ESSENCE), which gathers personally identifiable information from emergency rooms, health plans, clinical laboratories, 911 calls, pharmacies, and veterinary clinics in an effort to discern unusual or suspicious symptoms and events.[122] The Enhanced Border Security and Visa Entry Reform Act of 2002 requires aircrafts and sea vessels to submit departure and arrival manifests indicating the names of all alien passengers,

---

> usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime. . . . When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or Government enforcement agent . . . .

Jackson then went on to list the "exceptional circumstances in which, on balancing the need for effective law enforcement against the right of privacy, it may be contended that a magistrate's warrant for search may be dispensed with: when a "suspect was fleeing or likely to take flight"; "[t]he search was of . . . a movable vehicle"; or "evidence or contraband was threatened with removal or destruction." *Id.* at 15.

[122] *See* Katherine McIntire Peters, *Pattern Recognition*, Sept. 19, 2003, *available at* http://www.govexec.com/features/0903/0903s2.htm (describing ESSENCE). ESSENCE is a much reduced version of the maligned Total Information Awareness program, now labeled Terrorism Information Program, that was restricted by Congress in 2002. 10 U.S.C. § 2241 (limiting scope and appropriations for total information awareness program).

which can be combed for suspicious travel patterns.[123] The much more sophisticated Computer Assisted Passenger Prescreening System (CAPPS) purportedly combines airline passenger lists with travel reservations, rental car status, travel companions, and address.[124] Data mining comes in many forms, but all varieties have one thing in common: they rely on dragnet perusal of transaction information.

One way of analyzing the Fourth Amendment implications of data mining would be to focus on the nature of the records that are mined. Under this approach, if ESSENCE accesses the contents of personally identified medical records for criminal investigation purposes, its algorithm ought to identify only people who are highly likely to be perpetrators of crime, while if all of its information comes from "public" records or is composed of isolated catalogic sources, then its ability to identify criminals need not be as potent. A second way of analyzing data mining would be to look at the extent to which it aggregates information about the individuals it investigates and tags. If one accepts the concern about creation of "personality mosaics" described earlier, data mining would need a high hit rate to the extent it accumulates a significant amount of identifiable data about individuals, even if, as with CAPPS, all of the information is catalogic in nature.

Either way, data mining does not fare well. From what we know, the profiles used in the programs are very unlikely to identify even a small number of terrorists or other criminals. In other words, they may not even be successful enough to pass the relevance test (which requires that the investigative technique do better than chance), much less reach a level of success commensurate with reasonable suspicion or probable cause. Perhaps if such a data mining program relied only on a small amount of catalogic data to identify potential targets, it would be permissible under the interpretation of the Fourth Amendment put forward here.[125] But once government begins using multiple databases to put together detailed dossiers on the activities of its citizens, it would have to show more than just a possibility that something useful might turn up.

---

[123] 8 U.S.C. §1731(a)(2) (requiring the establishment of a database for all arrivals and departures).

[124] *See* Charu A. Chandrasekhar, *Flying While Brown: Federal Civil Rights Remedies to Post-9/11 Airline Racial Profiling of South Asians*, 10 ASIAN L.J. 215, 221 (2003) (describing a profile using roughly 40 items which, although secret, are likely to include those listed).

## IV. COUNTER-PROPOSALS

What does this set of proposals mean for our detective friend, described in Part I of this article? If he is investigating a particular person (the frequent flyer, the free-spender or the young Arab man), he needs a *Terry* order to access public records through Choicepoint or one of the other commercial data brokers. And he needs a warrant based on probable cause to access the contents of the suspect's financial, school, medical and similar personal records, as well as to obtain aggregated catalogic information such as addresses of the person's email messages. If instead he is engaging in event-based investigation, the nature of the records sought determines the justification needed. If, as in the hypotheticals described in Part I, the focus is store records (in an effort to track down a sniper-killer), or skydiving club membership lists and cookies of websites (in an effort to identify terrorists planning to bomb a mall), he would be on solid ground if this catalogic data is likely to increase the probability of identifying the perpetrators. If instead access is sought to the content of personal records or to catalogic data that implicates First Amendment interests, individualized suspicion would be required.[126]

---

[125] A recently released report by a Department of Defense advisory committee requires court approval of data mining that will obtain "personally identifiable information" from records not readily available to the public. *See* Report of the Technology and Privacy Advisory Committee, Safeguarding Privacy in the Fight Against Terrorism 49, 51 (March 2004). However, it requires the court to find only that the information obtained be "reasonably related" to the investigation purpose–a relevance standard?–and does not otherwise distinguish between types of records. *Id.* at 51-52. The report makes several good suggestions regarding "anonymizing" data, record-keeping and other means of monitoring data mining. *Id.* at 48-59.

[126] The analysis should not change if government seeks personal information from records acquired by a commercial data broker that has obtained the infor-

While this set of rules is not uncomplicated, it recognizes fewer types of authorizations than the current regime. The officer need merely make distinctions between personal and public records when conducting target-based transaction surveillance, and between content and catalogic data when conducting event-base surveillance. Moreover, since transaction surveillance should generally only proceed pursuant to court order, any confusion on the detective's part can be cleared up by a judge.

One can imagine numerous alternative methods of regulating transaction surveillance. Professor Daniel Solove has put forth the most coherent alternative to current law and the proposal presented here.[127] He points out that technology has made it easier both to maintain information about people and to aggregate it.[128] Thus, he proposes that, rather than attempt to figure out a privacy hierarchy and match authorization requirements to it (the proportionality approach that informs this article), we should adopt a uniform regulatory regime for government access to any "system of records."[129] Specifically, Solove proposes that, outside of emergency situations, government should not be able to obtain information in records–whether it is content or catalogic data, whether it is held by private or public agencies–unless it can obtain what he calls a "regulated subpoena."[130] To obtain such a subpoena the government would have to demonstrate it has probable cause to believe the person whose records are sought is involved in criminal activity, and that the specific records targeted are of "material importance" to the investigation, which he describes as a standard that is "slightly more permissive

---

mation from the original record-holders. Otherwise, much of this regulation could be avoided. Data does not become less personal simply because it has been shifted from one entity to another. The crucial questions are whether it is content or catalogic/organizational information, and whether it was originally collected for private or public purposes.

[127] Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002).

[128] *Id.* at 1090-95.

[129] *Id.* at 1152-59.

[130] *Id.* at 1164.

than that of a warrant," though more demanding than the relevance standard required for a subpoena (and, presumably, the reasonable suspicion required for a *Terry* order).[131] As with traditional subpoenas, the regulated subpoena would be challengeable by the target.[132]

Solove makes interesting arguments as to why his approach is superior to a proportionality approach. First, he points to the difficulty of differentiating between degrees of privacy and intimacy,[133] a difficulty illustrated by my attempts to distinguish content from catalogic information, personal from organizational records, and private from public records. Second, even if we could resolve these definitional problems, Solove believes that making privacy the linchpin of analysis is conceptually bankrupt. He notes, for instance, that we would never think of requiring the police to obtain a warrant in order to obtain a description of a suspect's genitals from his sexual partner, yet that information is probably as "private" as anything found in one's medical records.[134] Privacy, Solove argues, is a contextual concept that cannot form the basis for uniform regulation.[135] Rather, in the transaction surveillance setting, the focus should be whether the information is maintained in a system of records.[136] So, to return to his example, the police could interview the sexual partner without restriction, but would need a regulated subpoena to access the medical record of the suspect for the same information.

I agree with the premise of both of Solove's arguments, but am less persuaded that they lead to his conclusion. Solove is right that making the subtle distinctions demanded by a proportionality approach is difficult and can result in over or under protection of information at the margins. But requiring a uniform standard of probable cause for all record searches, as Solove would, provides far too much protection for some types of information. For instance, data mining of any sort would be almost impossible; if probable cause were required, the sniper-killer and terrorist investigations described above would probably never get off the ground. Or imagine that police want to find out from the phone company who called a murder victim in the two weeks prior to the murder (a scenario often depicted on TV shows like Law & Order). While they would certainly be able to demonstrate the relevance of this catalogic data, they would not have probable cause with respect to any of the callers, and thus would not be able to obtain the regulated subpoena for the phone company's records that Solove would demand. Creating a hierarchy of privacy, as tricky as it is, is important as a means of enabling the balancing of government and individual interests that the Supreme Court has sanctioned since the 1960s.[137]

---

[131] *Id.* at 1164-65.

[132] *Id.* at 1165.

[133] *Id.* at 1152-53.

[134] *Id.* at 1154.

[135] *Id.* at 1153-54. Solove develops this point in much more detail in Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1088-99 (2002).

[136] Solove, *supra* note 127, at 1157 ("Focusing on 'systems of records' targets the type of information flow that raises concern. Because the problem of modern government information-gathering is caused by the increasing dossiers maintained in private sector record systems, the architecture targets those third parties that store data in record systems.").

I also agree that the extent to which we are willing to protect private information is contextual, as Solove's example of the sexual partner interview demonstrates. However, that conclusion does not mean that privacy should be discarded as the baseline consideration in determining the government's authority to obtain information about its citizens. The reason we should treat interviews differently from records requests is not because privacy somehow is irrelevant in the former situation, but because the target's interest in privacy is countered by an even stronger interest–the third party's autonomy. Human information sources, such as the sexual partner, should have a right to decide what to do with the information they possess; in such cases, the subject's privacy interest is outweighed by the source's autonomy interest.[138] When the third party is an impersonal record-holder, on the other hand, concerns about denigrating "personhood" through limitations on when information may be revealed are non-existent.[139] It is the absence of a legitimate third party interest in surrendering the target's private information, not the bare fact that the information happens to reside in a record, that distinguishes the records request scenario from the interview setting.

---

[137] *See* Camara v. Mun. Ct., 387 U.S. 523, 536-37 (1967) ("[T]here can be no ready test for determining reasonableness other than by balancing the need to search against the invasion which the search entails.").

[138] Mary Irene Coombs, *Shared Privacy and the Fourth Amendment, or The*

These considerations lead me to conclude, contrary to Solove, that privacy concerns should be the fundamental consideration in analyzing transaction surveillance. While information generally should be accorded privacy protection when recorded, the extent of that protection should depend on the degree of privacy associated with the information, not simply on whether it exists in record form. Thus, some transactional information–i.e., that found in truly public records and catalogic data–should be accessible on less than probable cause.

Another alternative to the proportionality approach advanced here evades the issue of whether it is under or over protective of privacy by asserting that it focuses on the wrong sort of privacy invasion. Professor William Stuntz concedes that "secret searches" of our transactional information create risks that "are worth worrying about."[140] But he contends that we would not be particularly bothered by easy government access to such information *if* we never find out it has occurred except in connection with prosecutions for serious

---

*Rights of Relationships*, 75 CAL. L. REV. 1593, 1643-44 (1987).

[139] For further development of this point, see Slobogin, *supra* note 89, at 834-35. Of course, the employees of the record-holder might want to reveal private information. *See, e.g.*, Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949, 1013 (1996) ("As the president of the United States Telephone Association put it in explaining that telephone companies are interested in acceding to law enforcement requests for assistance, the companies want to be 'good local citizen[s].'"). But limiting that ability is not denying the employee's "personhood," because the information is maintained by the institution, not the person.

[140] William J. Stuntz, *Local Policing After the Terror*, 111 YALE L.J. 2137, 2181 (2002).

crime.[141] In other words, covert access to and stringent control over use of transaction information should permit relaxation of the rules as to how we obtain it.

This ignorance-is-bliss notion is superficially attractive. But limiting information flow, which is essential to Stuntz' scheme, can be very difficult. The notion that data gathered by law enforcement will be restricted to a small group of government employees is particularly naive in the wake of 9/11, when literally hundreds of thousands of law enforcement officers are charged with fighting "terrorism," an amorphous threat to say the least.[142] And ensuring that the information government officials acquire through covert surveillance is used only for the purpose of prosecuting serious crime could be equally difficult, precisely because the surveillance is covert.[143] Finally, abandoning all suspicion requirements, as Stuntz would do, virtually guarantees that data would be gathered about large numbers of innocent people, which in turn is likely to increase the chances of government files containing misleading information about its citizens.[144]

Even if the information gathered is somehow confined to a limited and discrete group and is not misused or inaccurate in any way, routine suspicionless and covert transaction surveillance can eat away at whatever trust is left between government and its citizenry. As I wrote in a discussion of Stuntz' proposal in the context of public camera surveillance:

---

[141] *Id.* at 2184-85.

[142] *See generally*, Gabriel Soll, *Terrorism: The Known Element No One Can Define*, 11 WILLAMETTE J. INT'L L. & DISP. RESOL. 123 (2004). *See also* Peter Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1371 (2004) (stating that "the history of previous cycles shows the temptation of surveillance systems to justify an ever-increasing scope of activity, in the hopes that just a little bit more surveillance will catch the terrorists or prevent an attack").

[143] *Id.* at 1366 (discussing "a long-run concern that secret . . . orders" allowing "access to entire databases of records . . . will be used expansively to intrude into a wide array of domestic matters").

[144] The recent exemption of the FBI's Central Records System database from the provision in the Privacy Act that requires government records to be accurate, 68 Fed. Reg. 14140 (Mar. 24, 2003) (to be codified as 28 C.F.R. pt. 16), will not help matters.

> once the public becomes aware that random covert surveillance is occurring, as it inevitably would after a few prosecutions in which the covertly gleaned information is used, the panoptic effect of this regime will be greater than occurs with overt [surveillance]. . . . [W]e would assume that secret surveillance was pervasive, not just incidental. . . . Probably no passage in Orwell's novel *1984* is more chilling than the [following]: "there was of course no way of knowing whether you were being watched at any given moment. . . It was even conceivable that they watched everybody all the time."[145]

With the power of today's computers, government could monitor the transactions of everybody, all the time. A regulatory regime that explicitly *endorsed* that sort of process would destroy any sense of security people might have in today's technological society. Indeed, if government is to be allowed to find out details of our lives whenever it is interested in doing so, we would probably be more comfortable knowing precisely when the surveillance is occurring, rather than being left in the dark.[146]

A final means of regulating transaction surveillance is to leave the task up to the legislature, specifically Congress. Professor Orin Kerr has made the most powerful argument for this approach.[147] He correctly points out that congressional statutes have provided more protection against transaction surveillance than the Supreme Court's construal of the Fourth Amendment in cases like *Miller*,[148] and that, in theory, legislatures are better equipped than courts to craft clear rules governing transaction surveillance in an era of rapidly changing, complicated technology.[149] But his arguments fail to negate two crucial facts, documented in this article, about the transaction surveillance rules that Congress has enacted to date: The rules have *not* been particularly clear[150] and, more importantly, they do not provide *adequate* protection against government access to our personal records. Especially in the wake of 9/11, Congress is unlikely to alter its stance unless the courts, relying on the Fourth Amendment, nudge it in the right direction.

---

[145] Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 305 (2002); *see also* The Council for Excellence in Government, From the Home Front to the Front Lines, America Speaks Out About Homeland Security 6 (March 2004) *available at* http://www.excelgov.org (poll indicating that 72% of Americans have "some" or "very little" trust in the government to "use personal information appropriately").

[146] *Cf.* DAVID BRIN, THE TRANSPARENT SOCIETY (1998) (arguing that "watching the watchers" is the only workable method of regulating government intrusion in the age of technology).

[147] Orin S. Kerr, *The Fourth Amendment and the New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004).

[148] *Id.* at 856.

Will the courts be willing to engage in such nudging? Certainly, *Miller*, *Smith* and like cases indicate that the Supreme Court is reticent about doing so. But in more recent decisions applying the "special needs" doctrine, which raises parallel issues, the Court has backed off its nonchalant attitude toward nontraditional searches and seizures. In *Ferguson v. City of Charleston*,[151] the Court declared unconstitutional a policy that authorized hospital drug testing of pregnant patients for the purpose of detecting illegal drug use, over a dissent by Justice Scalia arguing that, under *Miller*, the patients voluntarily assumed the risk the results of such tests would be used for investigative purposes.[152] The majority in *Ferguson* ignored Scalia's complaint, reasoning that a reasonable patient would assume the test results would be used for diagnostic purposes and that otherwise they would be kept confidential.[153] In both *Ferguson* and *Indianapolis v. Edmond*,[154] which held invalid a roadblock set up to interdict narcotics, the Court also emphasized that individualized cause requirements may not be relaxed if the only "special need" pleaded by the government is a "general interest in law enforcement."[155]

---

[149] *Id.* at 857-87.

[150] Kerr himself has noted that much of the legislation governing transaction surveillance is complicated. *See, e.g.,* Kerr, *supra* note 90, at 1208 ("[C]ourts, legislators, and even legal scholars have had a very hard time making sense of the [Stored Communications Act of ECPA]."); Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 820 (2003) (the "law of electronic surveillance is famously complex, if not entirely impenetrable.").

[151] 532 U.S. 67 (2001).

[152] *Id.* at 95 (Scalia, J., dissenting) ("Until today, we have *never* held—or even suggested—that material which a person voluntarily entrusts to someone else cannot be given by that person to the police, and used for whatever evidence it may contain.").

[153] *Id.* at 78 ("The use of an adverse test result to disqualify one from eligibili-

*Ferguson* signals that the Court is hesitant about granting the government an exemption from traditional Fourth Amendment standards simply because information relevant to a criminal investigation has been handed over to a third party (thus undermining *Miller*'s premise). And both *Ferguson* and *Edmond* suggest that strong government allegations that relaxation of those standards is necessary to detect criminal activity will not always prevail (thus undermining the "heightened need" rationale as a ground for reducing Fourth Amendment protections). These decisions provide a glimmer of hope that, when confronted with cases challenging subpoenas for personal records about medical treatment, personal finances and the contents of email messages, the Court will withdraw from its broad pronouncements in *Miller*. If it does so, further, more detailed rule-making along the lines suggested here might best be left to Congress, for the reasons Kerr suggests. The goal is meaningful protection of personal information. The source of that protection is not so important.

## CONCLUSION

Analysis of government surveillance has tended to focus on communications and physical surveillance. Yet transaction surveillance is at least as pervasive as these other types of

---

ty for a particular benefit, such as a promotion or an opportunity to participate in an extracurricular activity, involves a less serious intrusion on privacy than the unauthorized dissemination of such results to third parties. The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent.").

[154] 531 U.S. 32 (2000).

[155] *Ferguson*, 532 U.S. at 79; *Edmond*, 531 U.S. at 47 ("When law enforcement authorities pursue primarily general crime control purposes at checkpoints such as here, however, stops can only be justified by some quantum of individualized suspicion.").

investigative techniques, and can be as inimical to privacy interests. Public and private records contain information regarding virtually every aspect of our lives. In the past few decades, technology has made that information infinitely more easily aggregated and accessible.

Nonetheless, neither legislatures nor courts have evidenced much concern about transaction surveillance. Congress appears to think of transaction information as "business records," and thus at most entitled to the protection afforded by subpoenas, while the Supreme Court tells us we must assume the risk that record-holders will betray us. These positions ignore the obvious fact that medical, financial and other types of private and public records contain much personal information. They also fail to acknowledge that disclosure of that information to record-keepers–disclosure that those of us who live a modern lifestyle cannot avoid–is no different, in expectation of privacy terms, than communicating with others by phone or email or interacting with others inside one's home, both activities clearly protected by the Constitution. As Senator Sam Ervin recognized in 1974, "[g]overnment has an insatiable appetite for power, and it will not stop usurping power unless it is restrained by laws they cannot repeal or nullify."[156] When it comes to transaction surveillance, only the Fourth Amendment provides that type of restraint.

---

[156] Introductory Remarks of Senator Sam J. Ervin on S. 3418, H.R. REP. NO. 93-1416 (1974), *reprinted in* U.S. CONGRESS, LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974, at 3-8 (1976).

# THE FOURTH AMENDMENT ASPECTS OF COMPUTER SEARCHES AND SEIZURES: A PERSPECTIVE AND A PRIMER

*Thomas K. Clancy*[*]

I. Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 195
II. The Nature of Computer Searches: Searches for Data . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 196
  A. Document Searches . . . . . . . . . . . . . . . . . . . . . . 196
  B. Views Whether Computer Data are Documents . 197
    1. Data Are Forms of Records/Container Analogy . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 197
    2. Rejection of the Document Search and Container Analogy: A "Special Approach" . . . . 202
    3. Discussion of the Premises of the "Special Approach" . . . . . . . . . . . . . . . . . . . . . . . . . . 205
      a. Should File Names or Types Limit the Scope of a Search? . . . . . . . . . . . . . . . . . . . . . . . . 206
      b. Do Technological Search Programs Make the File Cabinet Analogy Inadequate? . . . . . . . 210
      c. Does the Nature or Amount of Material Make Computers Different From Other Containers? . . . . . . . . . . . . . . . . . . . . . . . 216

---

[*] Director, National Center for Justice and the Rule of Law, and Visiting Professor, University of Mississippi School of Law. I thank Don Mason and Marc Harrold for their comments on an earlier draft of this article. The National Center for Justice and the Rule of Law is supported by Grant No. 2000-DD-VX-0032 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in this article are those of the author and do not represent the official position of the United States Department of Justice.

            d. Limitations Based on Search Execution Procedures in Warrants . . . . . . . . . . . . . . . 218
III. Selected Fourth Amendment Applicability Issues . . . 220
  A. Expectation of Privacy Analysis . . . . . . . . . . . . . 220
    1. In General . . . . . . . . . . . . . . . . . . . . . . . . . . 220
    2. The Location of the Computer—In General . 221
    3. Data on Work Computers—Governmental Employer . . . . . . . . . . . . . . . . . . . . . . . . . . . 222
    4. Data on Work Computers—Private Employer 224
    5. Information Obtained from Third Parties . . . 225
    6. Joint Users; Password Protected Files . . . . . 227
  B. Private Searches and Seizures . . . . . . . . . . . . . . 228
    1. In General . . . . . . . . . . . . . . . . . . . . . . . . . . 228
    2. Government Agents . . . . . . . . . . . . . . . . . . 228
    3. Replication and "Context" Issues . . . . . . . . . 233
IV. Selected Satisfaction Issues . . . . . . . . . . . . . . . . . . 244
  A. Probable Cause . . . . . . . . . . . . . . . . . . . . . . . . . 244
  B. Consent . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 253
    1. In General . . . . . . . . . . . . . . . . . . . . . . . . . . 253
    2. Scope of Consent . . . . . . . . . . . . . . . . . . . . . 254
    3. Third Party Consent . . . . . . . . . . . . . . . . . . . 256
  C. Particularity Claims . . . . . . . . . . . . . . . . . . . . . 258
    1. In General . . . . . . . . . . . . . . . . . . . . . . . . . . 258
    2. Varieties of Computer Searches . . . . . . . . . . 259
      a. Searches for Computer Equipment . . . . . 260
      b. Searches for Data . . . . . . . . . . . . . . . . . . 261
  D. Plain View . . . . . . . . . . . . . . . . . . . . . . . . . . . . 262
  E. Execution Issues . . . . . . . . . . . . . . . . . . . . . . . . 264
    1. On-site/Off-site Searches; Intermingled Documents . . . . . . . . . . . . . . . . . . . . . . . . . . 264
    2. Use of Experts . . . . . . . . . . . . . . . . . . . . . . . 269
    3. Deleted Files . . . . . . . . . . . . . . . . . . . . . . . . . 269
V. Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 271

## I. INTRODUCTION

This article is called a "primer" because it outlines the application of Fourth Amendment principles to the search and seizure of computers and the digital information that is stored in them. It does not purport to address every Fourth Amendment issue that may arise in the computer context because, for many issues, the mere fact that a computer is involved does not change the analysis. Instead, it focuses on situations that are influenced by the fact that the object to be searched and seized is a computer or the data stored on it. Like a traditional primer, this article reports how courts have addressed Fourth Amendment applicability and satisfaction issues in the computer context.

A primer is generally thought of as not espousing a point of view. This article, however, departs from that role in two important respects. First, in discussing the nature of computer and digital evidence searches and seizures, it rejects the view that those intrusions require a "special approach," that is, that unique Fourth Amendment rules are needed to regulate them; instead, this article adopts the view that computers are containers and the data they contain are mere forms of documents. This is to say that the principles applicable to document searches have equal application to electronic data searches. Second, it rejects expansion of the private search doctrine, used by some courts, which permits government agents to open data files that had not been opened during a preceding private party search and still not be a search within the meaning of the Fourth Amendment based on the theory that the "context" in which the file was found negated any reasonable expectation of privacy. Underlying both of these points of view is the perspective that a computer is a container of containers of documents, that is, each individual file is a separate container–just like each manila file in a filing cabinet is a container–that requires a separate opening to determine what is inside. This is to say that the mere fact that an item to be searched or seized is electronic evidence does not fundamentally change the Fourth Amendment analytical structure that governs.

## II. The Nature of Computer Searches: Searches for Data

There are two principal approaches to searches involving electronic data stored on computers. One view asserts that a computer is a form of a container and that the data in electronic storage are mere forms of documents. A second view maintains that searches for data require a "special approach," requiring unique procedures and detailed justifications. This article concludes that the first view is correct: computers are containers. As with all containers, they have the ability to hold physical evidence, including such items as wires, microchips, and hard drives. They also contain electronic evidence, that is, a series of digitally stored 0s and 1s that, when combined with a computer program, yield such items as images, words, and spreadsheets. Accordingly, the traditional standards of the Fourth Amendment regulate obtaining the evidence in containers that happen to be computers.

### *A. Document Searches*

In *Andresen v. Maryland*,[1] the Supreme Court outlined the broad parameters of a permissible records search. In upholding the search of an office for documents that sought evidence of the crime of false pretenses by an attorney involved in real estate settlement activity, the Court asserted:

> Under investigation was a complex real estate scheme whose existence could be proved only by piecing together many bits of evidence. Like a jigsaw puzzle, the whole "picture" of petitioner's false-pretense scheme . . . could be shown only by placing in the proper place the many pieces of evidence that, taken singly, would show comparatively little. The complexity of an illegal scheme may not be used as a shield to avoid detection when the State has demonstrated probable cause to believe that a crime has been committed and probable cause

---

[1] 427 U.S. 463, 479-80 (1976).

> to believe that evidence of this crime is in the suspect's possession.[2]

Although authorizing a broad document search, the Court observed:

> We recognize that there are grave dangers inherent in executing a warrant authorizing a search and seizure of a person's papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable. In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized. Similar dangers, of course, are present in executing a warrant for the "seizure" of telephone conversations. In both kinds of searches, responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.[3]

Several of the themes articulated by *Andresen* have been applied by lower courts to searches of computers for data. Those considerations include the complexity of the crime, whether innocuous files can be examined, and minimization procedures to reduce the intrusion upon the individual's protected interests. Antecedent to those themes, however, is the debate whether *Andresen's* framework for document searches is applicable to computer searches.

### B. *Views Whether Computer Data Are Documents*

#### 1. Data are Forms of Records/Container Analogy

Many courts view data in computer storage as a form of a document. Hence, a warrant that authorizes a search for "writings" or "records" permits a search of computer files.[4] This is to say that the government need not know the exact "form that records may take."[5] Indeed, this view asserts that there is "no principled distinction between records kept electronically and those in paper form"[6] and, hence, there is "no justification for favoring those who are capable of storing their records on computer over those who keep hard copies of their records."[7] In both instances, consistent with *Andresen*, "innocuous documents may be scanned to ascertain their relevancy"[8] in "recognition of 'the reality that few people keep documents of their criminal transactions in a folder marked '[crime] records.'"[9]

---

[2] *Id.* at 480 n.10.

[3] *Id.* at 482 n.11.

[4] *See* United States v. Hunter, 13 F. Supp. 2d 574, 581 (D. Vt. 1998) (warrant authorizing search for "records" permitted search of "computers, disks, and similar property"); United States v. Musson, 650 F. Supp. 525, 531 (D. Colo.

Courts adopting this view have often analogized computers to filing cabinets or to containers:

> [The police] may search the location authorized by the war-

---

1986) (seizure of computer diskettes approved under a warrant authorizing the seizure of "any records or writings of whatsoever nature showing any business or financial transactions"); Frasier v. State, 794 N.E.2d 449, 454, 460 (Ind. Ct. App. 2003) (warrant that authorized search of "notes and or records" of marijuana sales permitted police to examine computer files); People v. Gall, 30 P.3d 145, 153 (Colo. 2001) (when warrant authorized seizure of "written and printed material" indicating an intent to do physical harm to a person or building pursuant to an investigation of a conspiracy to murder and use explosives against a facility, seizure of computers permissible because they were "reasonably likely to serve as 'containers' for writings, or the functional equivalent of 'written or printed material'"); People v. Loorie, 630 N.Y.S.2d 483, 486 (County Ct. 1995) (warrant authorizing search for "records" permitted search of computer files); *cf.* United States v. Triumph Capital Group, Inc., 211 F.R.D. 31 (D. Conn. 2002) (warrant authorizing search for "file records" included text, remnants, and fragments of deleted files); United States v. Harding, 273 F. Supp. 2d 411, 425 (S.D.N.Y. 2003) (because photographs may be taken by digital or film cameras and can be scanned if initially captured by film, a warrant authorizing the police to search for "photographs" allowed agents to open and inspect graphical image files on a zip disk).

[5] United States v. Gawrysiak, 972 F. Supp. 853, 861 (D.N.J. 1997) (approving of warrant to search business office for evidence of fraud), *aff'd,* 178 F.3d 1281 (3d Cir. 1999); *accord* United States v. Henson, 848 F.2d 1374, 1383 (6th Cir. 1988).

[6] United States v. Lievertz, 247 F. Supp. 2d 1052, 1063 (S.D. Ind. 2002).

[7] United States v. Hunter, 13 F. Supp. 2d 574, 584 (D. Vt. 1998).

[8] *Id.* at 582; *accord* United States v. Gray, 78 F. Supp. 2d 524, 528 (E.D. Va. 1999).

[9] United States v. Hunter, 13 F. Supp. 2d 574, 582 (D. Vt. 1998) (quoting United States v. Riley, 906 F.2d 841, 845 (2d Cir. 1990)); *accord* United States v. Maali M., 346 F. Supp. 2d 1226, 1265 (M.D. Fla. 2004).

> rant, including any containers at that location that are reasonably likely to contain items described in the warrant. . . . This container rationale is equally applicable to nontraditional, technological "containers" that are reasonably likely to hold information in less tangible forms. Similarly a warrant cannot be expected to anticipate every form an item or repository of information may take, and therefore courts have affirmed the seizure of things that are similar to, or the "functional equivalent" of, items enumerated in a warrant, as well as containers in which they are reasonably likely to be found.[10]

Following this view, computers have been said to be "reasonably likely to serve as 'containers' for writings, or the functional equivalent of 'written or printed material.'"[11] This is despite the recognition that computer file searches present "a heightened degree" of intermingling of relevant and irrelevant material: "[t]oday computers and computer disks store most of the records and data belonging to businesses and attorneys."[12]

Accepting this view does not mean that wholesale searches of data on computers are permitted.[13] Instead, the courts look to traditional means to limit the scope of document searches, such as the nature of the criminal activity alleged[14] or the nature of the objects sought.[15] For example, searches of computers for evidence of child pornography and other sexual exploitation of children make up a shockingly large percentage of the decided cases; in response to particularity challenges in these cases, courts focus on the sufficiency of the allegations of criminal conduct[16] or the description of the objects[17] sought.

---

[10] People v. Gall, 30 P.3d 145, 153 (Colo. 2001) (citations omitted); *see also* United States v. Al-Marri, 230 F. Supp. 2d 535, 541 (S.D.N.Y. 2002) (a computer is a form of a container); People v. Loorie, 630 N.Y.S.2d 483, 486 (County Ct. 1995) (same); United States v. Barth, 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998) (same).

[11] People v. Gall, 30 P.3d 145, 153 (Colo. 2001).

[12] United States v. Hunter, 13 F. Supp. 2d 574, 581, 583 (D. Vt. 1998).

[13] The "container," however, must be properly defined. *See infra* notes 139-82 and accompanying text.

[14] *See* Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (warrants seeking subscriber information in obscenity investigation requiring that communications and computer records pertain to the listed offenses were as particular as circumstances permitted); United States v. Kow, 58 F.3d 423, 427 (9th Cir. 1995) (one way to make warrant particular is to specify suspected criminal conduct being investigated but warrant invalid when it authorized "the seizure of virtually every document and computer file" without indicating how items related to suspected crime); United States v. George, 975 F.2d 72, 76 (2d Cir. 1992) ("Mere reference to 'evidence' of a violation of a broad criminal statute or general criminal activity provides no readily ascertainable guidelines for the executing officers as to what

---

items to seize."); Lafayette Academy, Inc. v. United States, 610 F.2d 1, 5-6 (5th Cir. 1979) (warrant that resulted in removal of four or five truckloads of documents and computer-related materials violated the particularity requirement when, *inter alia*, it did not specify type of fraud under investigation); United States v. Hunter, 13 F. Supp. 2d 574, 582-83 (D. Vt. 1998) (discussing limitations on scope of search involving money laundering scheme); *In re* Search Warrant for K-Sports Imports, Inc., 163 F.R.D. 594, 597-98 (C.D. Cal. 1995) (warrant for "all computer records and data," without limiting to crime under investigation, violated particularity requirement); State v. Askham, 86 P.3d 1224, 1227 (Wash. App. 2004) (warrant sufficiently particular when it names crime under investigation or when it describes in "some detail" suspected criminal activity; hence, when accused suspected of using computer to make threats and false accusations and warrant details the type of text files and web sites to be searched that could have been used to conduct that activity, it was sufficient); United States v. Longo, 70 F. Supp. 2d 225, 251 (W.D.N.Y. 1999) (warrant that authorized search of hard drive and any data disks for "two documents, one a promissory note, entitled TGL-003, contained within the directory labeled MISC, and a purchase agreement entitled 911, contained in the directory entitled IMF" specifically described area to be searched); State v. Nuckolls, 617 So. 2d 724, 726 (Fla. App. 1993) (warrant seeking records of used car business charged with forgery, odometer tampering, and other criminal violations sufficient when it authorized seizure of "[d]ata stored on computer, including, but not limited to, magnetic media or any other electronic form, hard disks, cassettes, diskettes, photo optical devices and file server magnetic backup tapes" because it left nothing to discretion of officers executing warrant).

[15] *See* United States v. Thorn, 375 F.3d 679, 684-85 (8th Cir. 2004) (warrant that authorized search and seizure of electronic storage media containing images of minors engaged in sexual acts allowed examination of contents of various computer-related media); United States v. Wong, 334 F.3d 831, 837-38 (9th Cir. 2003) (warrant authorizing search of computer to "obtain data as it relates to this case" sufficiently particular when combined with warrant's list of items sought in house); State v. One Pioneer CD-ROM Changer, 891 P.2d 600, 604 (Okla. Ct. App. 1995) (seizure of computer system permissible under warrant authorizing seizure of "equipment . . . pertaining to the distribution or display of pornographic material in violation of state obscenity laws"); Schalk v. State, 823 S.W.2d 633, 644 (Tex. Crim. 1991) (in theft of trade secrets prosecution, "magnetic tapes" that contained or were reasonably believed to contain stolen data and/or files sufficiently described items to be seized).

[16] *See* United States v. Meek, 366 F.3d 705, 714-15 (9th Cir. 2004) (warrant sufficient to search for crime involving use of Internet when it listed numerous

---

items relating to seduction and sexual exploitation of children: sexually explicit material or paraphernalia used to lower inhibition of children, sex toys, photography equipment, child pornography, as well as material related to past molestation such as photographs, address ledgers including names of other pedophiles, journals of sexual encounters with children, computer equipment, information on digital and magnetic storage devices, computer printouts, computer software and manuals, and documentation regarding computer use); United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000) (upholding validity of search of computer equipment and files because warrant limited search to evidence of crimes involving sexual exploitation of children); United States v. Gleich, 293 F. Supp. 2d 1082, 1088 (D.N.D. 2003) (warrant authorizing search of computer for photographs, pictures, visual representations, or videos that included sexual conduct by minor, as defined by North Dakota statute, met particularity requirement), *aff'd,* 397 F.3d 608 (8th Cir. 2005); United States v. Hall, 142 F.3d 988, 996-97 (7th Cir. 1998) (when items listed in warrant qualified by phrases that items sought were related to child pornography, particularity requirement satisfied); United States v. Clough, 246 F. Supp. 2d 84, 87-88 (D. Me. 2003) (warrant in child pornography case authorizing search of "text documents" and "digital images" violated particularity requirement when there were "no restrictions on the search, no references to statutes, and no references to crimes or illegality"); State v. Wible, 51 P.3d 830, 837 (Wash App. 2002) (warrant particular when it limited search to images of children engaged in sexually explicit activity as defined by child pornography statute); *cf.* United States v. Maxwell, 45 M.J. 406, 420 (C.A.A.F. 1996) (rejecting challenge to warrant that included persons who could have unknowingly received child pornography in their email mailboxes because to narrow the field to only those who had knowingly received images would have required advance search of mailboxes to ascertain if files had been opened).

[17] *See* United States v. Gleich, 397 F.3d 608, 612 (8th Cir. 2005) (warrant authorizing search of home and personal computer for "photographs, pictures, visual representations or videos in any form that include sexual conduct by a minor" permitted search of all three computers in house); *Thorn*, 375 F.3d at 685 (warrant that authorized search and seizure of electronic storage media containing images of minors engaged in sexual acts sufficed to provide authority to examine contents of various computer-related media); United States v. Campos, 221 F.3d 1143, 1147-48 (10th Cir. 2000) (warrant particular when it authorized, *inter alia*, seizure of computer equipment that may be used to depict or distribute child pornography); United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999), *cert. denied,* 527 U.S. 1011 (1999) (upholding warrant issued for "[a]ny and all computer software and hardware, . . . computer disks, disk drives" in house of woman suspected of sending and receiving child pornography over Internet); Davis v. Gracey, 111 F.3d 1472, 1479 (10th Cir. 1997) ("equipment . . . pertaining to the distribution or display of pornographic material" was sufficiently precise to limit search to computer equipment connected with that criminal activity); United States v. Albert, 195 F. Supp. 2d 267, 275-76 (D. Mass. 2002) (warrant particular when it authorized search and seizure of computer, disks, software, and storage devices when there was probable cause to believe that the computer contained more than 1000 images of child pornography, given that the "search and seizure

### 2. Rejection of the Document Search and Container Analogy: A "Special Approach"

Some authorities reject the container analogy and view searches for data on a computer much differently than paper document searches.[18] The leading case, *United States v. Carey,*[19] espouses the view that law enforcement officers must take a "special approach"[20] to the search of data contained on

---

of the computer and its related storage equipment was the only practical way to obtain the images"); United States v. Allen, 53 M.J. 402, 407-08 (C.A.A.F. 2000) (warrant particular when it authorized search for computer files relating to nude photographs of juveniles, Internet locations of such material, or lists of such files); State v. Wible, 51 P.3d 830, 836-37 (Wash. App. 2002) (warrant for child pornography satisfies particularity requirement if it limits seizable items by specifying type of material that qualifies as child pornography); State v. Maxwell, 825 A.2d 1224, 1234 (N.J. Super. 2001) (in case involving use of telephone to call child victims of sexual assault, warrant that authorized search of computer for "computer address books" valid); State v. Patscheck, 6 P.3d 498, 500-01 (N.M. App. 2000) (in prosecution for sexual offenses against children, warrant that specified computer to be searched for "pornographic movies" valid); State v. Lehman, 736 A.2d 256, 260-61 (Me. 1999) (warrant not overbroad when it authorized seizure of all computer-related equipment in suspect's house when police knew only that the images of sexually exploited girls were taken by a digital camera and downloaded to a computer); *cf.* United States v. Lamb, 945 F. Supp. 441, 457-59 (N.D.N.Y. 1996) (warrant satisfied particularity requirement in child pornography case seeking subscriber information and electronic mail messages sent to and received by 78 individuals from Internet service provider when messages were instrumentalities of crime used by child pornography traffickers to locate and communicate with persons of like mind).

[18] *See* Raphael Winick, *Searches and Seizures of Computers and Computer Data,* 8 HARV. J.L. & TECH. 75, 110 (1994) ("An analogy between a computer and a container oversimplifies a complex area of Fourth Amendment doctrine and ignores the realities of massive modern computer storage."); *see also* Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. TECH. L. REV. 39, 60-63, 81-82 (2002) (setting forth some of the differences between searches of "paper documents and computer-generated evidence" and maintaining that courts should impose restrictions on computer searches such as limiting the search by file types, by requiring a second warrant for intermingled files, and by imposing time frames for conducting the search).

[19] 172 F.3d 1268 (10th Cir. 1999).

[20] *Id.* at 1275 n.7; *see also* People v. Gall, 30 P.3d 145, 160 (Colo. 2001) (Martinez, J., dissenting) ("Because computers process personal information and effects, they require heightened protection under the Fourth Amendment against unreasonable searches or seizures.").

computers and that the "file cabinet analogy may be inadequate."[21] This position is premised on the fact that "electronic storage is likely to contain a greater quantity and variety of information than any previous storage method."[22] As one judge has argued:

> A computer is fundamentally different from a writing, or a container of writings, because of its capacity to hold a vast array of information in many different forms, to sort, process, and transfer information in a database, to provide a means for communication via e-mail, and to connect any given user to the internet. A computer may be comprised of a wide variety of personal information, including but not limited to word processing documents, financial records, business records, electronic mail, internet access paths, and previously deleted materials. Because of these differences, the seizure of a computer raises many issues beyond those that might pertain to mere writings. . . .
>
> A "writing" is simply not particular enough to warrant a reasonable person to conclude that it includes a computer because a writing and a computer are two fundamentally different things, both in degree and in kind. . . . Moreover, Fourth Amendment analysis regarding the search and seizure of computers must be approached cautiously and narrowly because of the important privacy concerns inherent in the nature of computers, and because the technology in this area is rapidly growing and changing.[23]

Other arguments that searches of computers are different include the assertion that computers "present the tools to refine searches in ways that cannot be done with hard copy files. When confronting a file cabinet full of papers, there may be no way to determine what to seize without doing some level of review of everything in the cabinet"; in contrast, computer technology affords a variety of methods by which the government may tailor a search to focus on documents that evidence the alleged criminal activity.[24] Those methods, it has been asserted, include limiting searches by date range, doing key word searches, limiting searches by file type, and "focusing on certain software programs."[25]

---

[21] *Carey*, 172 F.3d at 1275.

[22] Winick, *supra* note 18, at 105; *see also In re* Search of 3817 W. West End, 321 F. Supp. 2d 953, 958-59 (N.D. Ill. 2004) (asserting that searches of computers require "careful scrutiny of the particularity requirement" because, *inter alia,* of the "extraordinary volume of information that may be stored").

[23] People v. Gall, 30 P.3d 145, 162-65 (Colo. 2001) (Martinez, J., dissenting).

Under this "special approach," courts have imposed several unique requirements: a search warrant seeking to seize computers or computer equipment must specify that it covers such items and the warrant must "include measures to direct the subsequent search of a computer."[26] Police officers may also have to limit the search by "observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory."[27] To restrict the scope of a search of a computer that contains intermingled documents, those rejecting the premise that computer searches are just another form of a document search maintain that merely obtaining a warrant to search for specified items is insufficient.[28] Instead,

---

[24] *In re* Search of 3817 W. West End, 321 F. Supp. 2d at 959.

[25] *Id.*

[26] People v. Gall, 30 P.3d 145, 164-65 (Colo. 2001) (Martinez, J., dissenting); *see also In re* Search of 3817 W. West End, 321 F. Supp. 2d at 957 (maintaining that an issuing magistrate had authority to require government to follow "search protocol that attempts to ensure that the search will not exceed constitutional bounds").

[27] United States v. Carey, 172 F.3d 1268, 1276 (10th Cir. 1999); *see also* People v. Carratu, 755 N.Y.S.2d 800, 807-09 (N.Y. Sup. Ct. 2003) (stating that police did or did not have right under warrant to open computer file folders based on name associated with that folder); *In re* Grand Jury Subpoena Duces Tecum Dated November 15, 1993, 846 F. Supp. 11, 13 (S.D.N.Y. 1994) (based on government's concession, asserting that key word search of information stored on computer would reveal information likely to be relevant to grand jury investigation); People v. Gall, 30 P.3d 145, 166 (Colo. 2001) (Martinez, J., dissenting) ("[S]earches may be limited to avoid searching files not included in the warrant by 'observing files types and titles listed in the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory"); Winick, *supra* note 18, at 107 ("Once officers seize large quantities of computer memory, they have three methods of distinguishing relevant from irrelevant information. Officers can either read through portions of each file stored in the memory, conduct a key word search of the data stored on the disks, or print out a directory of the title and file type for each file on the disk.").

[28] The origin of the intermingled document doctrine can be traced to a non-

> [L]aw enforcement must engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant. Where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents. The magistrate should then require officers to specify in a warrant which type of files are sought.[29]

### 3. Discussion of the Premises of the "Special Approach"

As this section explains, I believe the "special approach" is misguided. It has no foundation in Fourth Amendment jurisprudence, even by analogy, given its essential postulate that computer technology is so fundamentally different from anything in the past. This postulate has been articulated to include several premises. First, technology not only creates a vastly different system of storage, information, and privacy concerns, it also affords ways to minimize intrusions. Because such methods are available, so the reasoning goes, they must be used. Second, computer abilities are fundamentally different than anything previously known to humankind, mandating rejection of the document and container doctrines that the Supreme Court has articulated to regulate those other types of searches. Third, because of the other premises, computer searches and

---

computer case, which involved a large volume of material. *See* United States v. Tamura, 694 F.2d 591, 595-97 (9th Cir. 1982) (government can avoid violating Fourth Amendment rights by sealing documents pending issuance of search warrant detailing further search); *see also* United States v. Shilling, 826 F.2d 1365, 1369 (4th Cir. 1987) (regarding file cabinets, government should adopt procedure outlined in *Tamura* and require subsequent search warrant). *But see* United States v. Hill, 322 F. Supp. 2d 1081, 1090 (C.D. Cal. 2004) (rejecting *Tamura* as applicable precedent because warrant permitted seizure of all storage media); David J.S. Ziff, Note, *Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant*, 105 COLUM. L. REV. 841, 858-61 (2005) (arguing inapplicability of *Tamura* to computer searches).

[29] *Carey*, 172 F.3d at 1275 (footnote omitted); *accord* United States v. Walser, 275 F.3d 981, 986-87 (10th Cir. 2001); United States v. Campos, 221 F.3d 1143, 1148 (10th Cir. 2000); Winick, *supra* note 18, at 105-07.

seizures require the courts to create special search execution rules. Each of these premises and the underlying postulate, I believe, are flawed. Instead, the proper view is that computer and electronic data searches are properly governed by traditional Fourth Amendment rules regulating containers and document searches.

### a. *Should File Names or Types Limit the Scope of a Search?*

An essential premise of the "special approach" is that file name labels or suffixes accurately indicate what the file contains.[30] As one commentator has asserted:

> Computer programs store information in a wide variety of formats. For example, most financial spreadsheets store information in a completely different format than do word processing programs. Similarly, an investigator reasonably familiar with computers should be able to distinguish database programs, electronic mail files, telephone lists and stored visual or audio files from each other. Where a search warrant seeks only financial records, law enforcement officers should not be allowed to search through telephone lists or word processing files absent a showing of some reason to believe that these files contain the financial records sought.[31]

In *Carey*, the principal case espousing this "special approach," the police had a warrant allowing them to search computer files for "names, telephone numbers, ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances."[32] During the course of the search, Detective Lewis came across files with sexually suggestive titles and the suffix "jpg."[33] Upon opening one of those files, Lewis observed child pornography. He subsequently downloaded numerous other "jpg" files and opened some of them, revealing additional child pornography. The "jpg" files featured sexually suggestive or obscene names, many including the word "teen" or "young."[34] Lewis testified that, until he opened each file, he really did not know its contents.[35] He claimed: "I wasn't conducting a search for child pornography, that happened to be what these turned out to be."[36] Although the trial court denied the motion without making any findings of fact, the appellate court reversed, imposing its own view of the evidence:

---

[30] *See Carey*, 172 F.3d at 1275 ("This is not a case in which ambiguously labeled files were contained in the hard drive directory. It is not a case in which the officers had to open each file drawer before discovering its contents."); People v. Carratu, 755 N.Y.S.2d 800, 807 (N.Y. Sup. Ct. 2003) ("[A] warrant authorizing a search of the text files of a computer for documentary evidence pertaining to a specific crime will not authorize a search of image files containing evidence of other criminal activity."); Amy Baron-Evans, *When the Government Seizes and Searches Your Client's Computer*, 27 CHAMPION 18 (2003) ("Fortunately, the technical means exist to search computers for particular information without rummaging through private information not described in a warrant. For example, in a typical white collar case, relevant files can be isolated and irrelevant ones avoided through keyword searches. In a child pornography case, the government can search for picture files without the need to look at any text file."). *Cf.* Commonwealth v. Hinds, 768 N.E.2d 1067, 1073 (Mass. 2002) (suggestive file names can create probable cause to search computer for child pornography).

[31] *See* Winick, *supra* note 18, at 108.

> [T]he case turns upon the fact that each of the files containing pornographic material was labeled "JPG" and most featured a sexually suggestive title. Certainly after opening the first file and seeing an image of child pornography, the searching officer was aware—in advance of opening the remaining files—what the label meant. When he opened the subsequent files, he knew he was not going to find items related to drug activity as specified in the warrant[.][37]

Putting aside the appellate court's disregard of its limited role in fact-finding, there are significant reasons to reject its position that a search be restricted by file names or file types. Professional investigators recognize that computer users attempt to conceal criminal evidence by storing it "in random order with deceptive file names," thus requiring a search of all the stored data to determine whether it is included in the warrant.[38] Indeed, others have asserted that "it is impossible to tell what a computer storage medium contains just by looking at it. Rather, one has to examine it electronically, using a computer that is running the appropriate operating system, hardware and software."[39] As one court has maintained:

---

[32] *Carey*, 172 F.3d at 1270.

[33] *Id.*

[34] *Id.* at 1271 n.3.

[35] *Id.* at 1271. Lewis stated, however, that image files could contain evidence pertinent to a drug investigation such as pictures of "a hydroponic growth system and how it's set up to operate" and that drug dealers often obscure or disguise evidence of their drug activity. *Id.* at 1270 n.2.

[36] *Id.* at 1271.

[37] *Id.* at 1274.

> [Defendant] claims that the search should have been limited to certain files that are more likely to be associated with child pornography, such as those with a ".jpg" suffix (which usually identifies files containing images) or those containing the word "sex" or other key words.
>
> Defendant's proposed search methodology is unreasonable. "Computer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent." Images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer.
>
> Forcing police to limit their searches to files that the suspect has labeled in a particular way would be much like

---

[38] United States v. Campos, 221 F.3d 1143, 1147 (10th Cir. 2000) (quoting affidavit); *see also* United States v. Maali M., 346 F. Supp. 2d 1226, 1265 (M.D. Fla. 2004) (expert explained that he could not rely on file names to determine what was responsive to warrant); EOGHAN CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME (2d ed. 2004) (describing a methodical data filtering process that includes several different tools, *id.* at 632-43, and observing that digital evidence analysis requires examiners to employ filtering procedures to find potentially useful data and that "[l]ess methodical data reduction techniques, such as searching for specific keywords or extracting only certain file types, may not only miss important clues but can still leave the examiners floundering in a sea of superfluous data", *id.* at 230); Michael G. Noblett, Mark M. Pollitt, & Lawrence A. Presley, *Recovering and Examining Computer Forensic Evidence*, 2 FORENSIC SCIENCE COMMUNICATIONS 7 (2000) at www.fbi.gov/hp/lab/fsc/backissue/oct2000/computer.htm (observing that there is "no such thing as generic computer science procedures" and that "evidence is likely to be significantly different every time a submission is received by the laboratory and will likely require an examination plan tailored to that particular evidence").

[39] United States v. Hill, 322 F. Supp. 2d 1081, 1088 (C.D. Cal. 2004).

> saying police may not seize a plastic bag containing a powdery white substance if it is labeled "flour" or "talcum powder." There is no way to know what is in a file without examining its contents, just as there is no sure way of separating talcum from cocaine except by testing it. The ease with which child pornography images can be disguised—whether by renaming sexyteenyboppersxxx.jpg as sundayschoollesson.doc, or something more sophisticated—forecloses defendant's proposed search methodology.[40]

Similarly, in *United States v. Gray*,[41] the court rejected the argument that an agent could not search files tagged with the "jpg" suffix, even though none of the materials covered by the warrant were believed to be pictures. The court reasoned:

> While the ".jpg" suffix generally denotes a picture file, there is no requirement that it do so, and, as a result, Agent Ehuan could not be certain that files with the ".jpg" suffix did not contain the materials for which he was authorized to search. Indeed, Agent Ehuan would have been remiss not to search files with a ".jpg" suffix simply because such files are generally pictures files, and he believed the NLM documents and hacker materials were more likely to be text files. He knew from his experience that computer hackers often intentionally mislabel files, or attempt to bury incriminating files within innocuously named directories. Indeed, in the course of his search of defendant's computer files, Agent Ehuan found some text files mixed in with picture files. This serves to underscore the soundness of the conclusion that Agent Ehuan was not required to accept as accurate any file name or suffix and limit his search accordingly.
>
> Defendant further argues that Agent Ehuan, having been alerted by the names of the "Teen" and "Tiny Teen" subdirectories, was looking for child pornography when he opened the two subdirectories. Agent Ehuan testified persuasively to the contrary; he stated that, while the names of the subdirectories were suspicious to him, he opened the "Teen" and "Tiny Teen" subdirectories in the course of a systematic search of the BBS

---

[40] *Id.* at 1090-91.

[41] 78 F. Supp. 2d 524 (E.D. Va. 1999).

> directory. In other words, Agent Ehuan did not target those particular subdirectories because of their names, and, at all times, he was searching for the materials that were the subject of the search warrant.[42]

These authorities support the conclusion that *Carey's* limitations on search authority based on file names or types do not comport with the ability of computer users to hide data in innocuously labeled files. Instead, the more sound approach, consistent with *Andresen*, is that "innocuous [computer files] may be scanned to ascertain their relevancy"[43] in "recognition of 'the reality that few people keep documents of their criminal transactions in a [computer file] folder marked '[crime] records.'''[44]

### *b. Do Technological Search Programs Make the File Cabinet Analogy Inadequate?*

Another premise of authorities rejecting the file cabinet analogy is that technological searches can be employed by the government to scan data held in electronic storage to reliably sort relevant information from information for which the government does not have probable cause to search. This is a technical question and not a legal one.

There are a variety of software programs that government investigators now routinely employ when searching for electronic evidence.[45] It has been recognized that "automated search techniques have inherent strengths and weaknesses:"

---

[42] *Id.* at 529-30; *see also* Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001) (agents could legitimately check contents of directories to see if contents corresponded with labels placed on directories; suspects "would otherwise be able to shield evidence from a search simply by 'misfiling' it in directory labeled 'e-mail'"); State v. Schroeder, 613 N.W.2d 911, 916 (Wis. App. 2000) (rejecting limitations on search based on file names and concluding that, during systematic search of all user-created files in executing search warrant for evidence of online harassment and disorderly conduct, opening file containing child pornography in plain view); United States v. Abbell, 963 F. Supp. 1178, 1201 (S.D. Fla. 1997) (upholding seizure of computer disks despite fact that they did not contain responsive name because seizing agents "were not required to accept labels as indicative of the disks' contents").

[43] United States v. Hunter, 13 F. Supp. 2d 574, 583 (D. Vt. 1998); *accord* United States v. Gray, 78 F. Supp. 2d 524, 528 (E.D. Va. 1999).

[44] *Hunter*, 13 F. Supp. 2d at 582 (quoting United States v. Riley, 906 F.2d 841, 845 (2d Cir. 1990)).

> The usefulness [of automated keyword searches] is limited to situations where there is some precise textual identifier that can be used as the search argument. Keyword searches are context insensitive, and cannot employ the discrimination used by a human investigator. If either the data encoding or the alleged criminal activity is complex in nature, human judgment will be required to determine the evidentiary value of specific electronic documents and whether the documents fall within the scope of the warrant.
>
> The benefits of electronic search techniques are that they are fast, accurate, and within the narrow scope of their capabilities. If the officers are searching for very specific information and know one or two exact phrases or words to search for, a comprehensive electronic search can be conducted in a matter of hours. For example, if the officers were searching for a copy of specific insurance claims or accounting records, and the officers knew with certainty that these records would contain specific phrases, numbers, or names, these records could be located very quickly. Once the appropriate electronic records were located, they could be copied on a file-by-file basis, in effect allowing seizure of only the files that fall within the scope of the warrant.
>
> By contrast, if the officers conducting the search do not have specific information (names, numbers, phrases) sufficient to allow an accurate identification of *all* relevant documents, electronic searches are far less useful. The use of common words or phrases as keywords may still help locate relevant evidence, but such searches yield a high number of false hits. False hits are documents that contain the searched—for term, but have no evidentiary value and are beyond the scope of the warrant.
>
> The usefulness of keyword searches is further diminished by the fact that such searches are context insensitive. Computer data is encoded. Many computerized documents require

---

[45] One commonly used tool is Encase, designed by Guidance Software. *See* www.guidancesoftware.com.

specialized software to read or render their contents comprehensible. Such software provides the *context* required to interpret electronic data. For example, the medical records, accounting data, and medical appointment logs in our hypothetical would most probably contain many abbreviations or coded values representing various medical procedures and associated charges. A record containing a patient's name, a numeric value of 1, a procedure code of 346 and a charge of 740000 might not seem suspicious. But if the numeric value 1 is a code that indicates that the patient is a male, and the medical procedure code of 346 identifies the operation as a hysterectomy, then the legitimacy of the $7400.00 charge is suspect. Without knowing the context of the numbers 1, 346, and 740000, the data represented cannot be evaluated for relevance.

The manner in which computer data is represented also limits the effective scope of automated search techniques. Many automated search tools are based on the detection of textual character strings embedded in documents. These techniques can only be applied to textual data, and not for pictures, diagrams, or scanned images. For example, a search for the word "submarine" would locate text that contained those characters, but it would fail to locate the scanned image of a submarine, a digital photo of the control tower, or even a scanned image or photo of the original document. The textual search would also fail to locate the desired document if it had been compressed, encrypted, or password protected. Depending on the software used for the search, it might or might not detect the word "submarine" in files that had been deleted.

Other types of searches depend on properly identifying documents by either document type or by file name. Searches by file *name* are unreliable because a user is free to name (or rename) files without regard to their content. Searches by file *type*, can be accomplished using specialized tools that identify files based on the "signature" associated with the program used to create the file. This technique can be used to identify or group files based on how data is represented. These tools can identify file format, but are not able to search *content*. Searches based on file type are not normally effective against files which have been encrypted, compressed, or password protected.[46]

This passage merely describes the current state of competition between criminal minds and government investigators. The ability to hide evidence in electronic storage constantly evolves and the government must keep pace or catch up.[47] There will always be a considerable amount of uncertainty at any given time whether any one search technique identifies with an acceptable degree of accuracy what a file contains without opening it.

A second question is a legal one: does the Fourth Amendment mandate that advanced technological search engines be used? If technology is constantly evolving–and it is, then the inquiry is a moving target. This is to say that law enforcement must always stay on the cutting edge of technological change and continually invest money and resources for new training and new equipment. Such a mandate would be, in my view, a form of a least intrusive means analysis.[48] Recourse to a least intrusive analysis is a persistent minority view of the Fourth Amendment's requirements.[49] This is despite the clear mandate from the Supreme Court that it is not an element of reasonableness.[50] Indeed, there is no support for such an analysis in the language of the Amendment or in the historical regulation of search and seizure powers.[51] A least intrusive means analysis first appeared in opinions during the Warren Court era and its advocates do not rely on historical precedent to support it. Rather, they argue that it is necessary to achieve equivalence of protection between Fourth Amendment rights and other guarantees of the Bill of Rights.[52] For example, one commentator has argued that "the rationale which is commonly offered for according a special status to first amendment liberties—that they created the environment necessary for other freedoms to flourish–is equally applicable to the fourth amendment."[53] Such broad brush analysis ignores important historical differences in constitutional rights and the language of the constitution. For example, the First Amendment's Speech

---

[46] Brenner & Frederiksen, *supra* note 18, at 60-62; *see also* SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 59 (rev. ed. 2002), at http://www.purl.access.gpo.gov/GPO/cps11361 [hereinafter CCIPS Manual] ("Even where a considerable amount is known about a system, the agents and technicians conducting a review of data often have to use a number of different techniques in order to thoroughly search a computer and its storage media. Sometimes, seemingly commonplace data or configurations cannot be copied, reviewed or analyzed by one search program or protocol, so another–or several different ones–must be tried. Keyword searches may not be possible until a careful review of a portion of the files is conducted; moreover, a careful data search may reveal other, otherwise unapparent aspects of how the system is used and data generated, accessed, transmitted and stored."); *id.* at 105 (discussing how it is necessary to have a "robust search strategy" that may require "a careful file-by-file review" because of, *inter alia*, the limitations of keyword searches, the use of code words in files, and unusual locations where the data may be stored on a computer); Orin Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 303 (2005) ("Existing technology simply gives us no way to know ahead of time where inside a computer a particular file or piece of information may be located."); EOGHAN CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME (2d ed. 2004) (describing a methodical data filtering process that includes several different tools, *id.* at 632-43, and observing that digital evidence analysis requires examiners to employ filtering procedures to find potentially useful data and that "[l]ess methodical data reduction techniques, such as searching for specific keywords or extracting only certain file types may not only miss important clues but can still leave the examiners floundering in a sea of superfluous data", *id.* at 230).

[47] *See, e.g.,* EOGHAN CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME 643 (2d ed. 2004) (discussing the challenges to investigators of compressed files, encrypted files, e-mails, and email attachments, which require a "combination of tools with different features").

---

[48] *See* Winick, *supra* note 18, at 108 ("[T]he government should bear a heavy burden in demonstrating that no less intrusive method is available to separate files falling within the scope of the warrant from files falling outside the scope of the warrant.").

[49] *See* Thomas K. Clancy, *Protective Searches, Pat-Downs, or Frisks?: The Scope of the Permissible Intrusion to Ascertain if a Detained Person is Armed*, 82 MARQ. L. REV. 491, 513-14 (1999) (collecting cases).

[50] *See id.* at 514-15 (collecting cases).

[51] *See, e.g.*, United States v. Koyomejian, 970 F.2d 536, 546 (9th Cir.) (Kozinski, J., concurring) (finding no support for a least intrusive means requirement in either the language of the Fourth Amendment or in the "two centuries of search and seizure caselaw" interpreting it), *cert. denied*, 506 U.S. 1005 (1992).

[52] *See* Nadine Strossen, *The Fourth Amendment in the Balance: Accurately Setting the Scales through the Least Intrusive Means Analysis*, 63 N.Y.U. L. REV. 1173, 1242 (1988); Scott E. Sundby, *A Return to Fourth Amendment Basics: Undoing the Mischief of Camara and Terry,* 72 MINN. L. REV. 383, 436-37 (1988) (arguing that a strict scrutiny-least intrusive means standard would "bestow preferred status upon the fourth amendment as a fundamental right").

[53] Strossen, *supra* note 52, at 1241 (footnote omitted).

Clause utilizes absolute language: "Congress shall make *no* law . . . abridging the freedom of speech." Given that absolute bar, as a general matter, it is appropriate that restrictions on speech should be subjected to a requirement of necessity, that is, that the government have a compelling interest and that the restriction be narrowly tailored to effectuate that interest.[54] Such close tailoring analysis is, however, inappropriate in the Fourth Amendment context, which, instead of barring governmental intrusions, requires only that the intrusion be reasonable. This is to say that reasonableness is a more forgiving concept than a least intrusive means analysis allows. In accordance with that mandate, the means need be only reasonably related to the justification for the intrusion.[55]

The proper question for searches of data stored on a computer–as with all questions of reasonableness–is whether the means chosen by the government to execute the search are reasonably related to the purpose of the search. This inquiry, in my view, does not mandate that the police utilize any specific technology or procedures at any given time, particularly where the state of technology creates uncertainty that the search would be effective if limited to certain means. Indeed, there is no parallel in Supreme Court jurisprudence limiting intrusions to means that might permit evidence to go undetected once it is determined that the police have a warrant to search based on probable cause to believe that the place to be searched contains evidence of a crime.[56]

---

[54] *See, e.g.*, Ashcroft v. American Civil Liberties Union, 542 U.S. 656 (2004) (looking to less restrictive alternatives to content-based restrictions on speech in context of Congressional attempts to protect minors from sexually explicit materials on Internet).

[55] *See* United States v. Gray, 78 F. Supp. 2d 524, 529 n.8 (E.D. Va. 1999) (police searching computers not obligated to conduct "the most technically advanced search possible"; instead, proper question is "whether the search, as conducted was reasonable").

[56] *See generally* Thomas K. Clancy, *The Fourth Amendment's Concept of Reasonableness*, 2004 UTAH L. REV. 977 (2004) [hereinafter Clancy, *Concept of Reasonableness*] (discussing the Supreme Court's reasonableness analysis). The Court has created a few unusual restrictions for probable-cause based intrusions due to heightened concerns for intrusions into the body and based on free-speech concerns. *See id.* at 1015-20. Certainly, the search of a computer is not analogous to

### *c. Does the Nature or Amount of Material Make Computers Different from Other Containers?*

A fundamental premise of the "special approach," which asserts that computers should be treated differently than other containers of evidence, is the belief that "electronic storage is likely to contain a greater quantity and variety of information than any previous storage method."[57] The premise does not dispute that, at the most basic level, a computer is a container of a variety of items, ranging from wires to hard drives, some of which hold (contain!) digital evidence. The underlying rationale seems to be nothing more than the fact that computers store such a vast amount of information of all sorts that the particular container called a computer becomes distinct from any previous container.

The Supreme Court at one point attempted to distinguish among types of containers in ranking expectations of privacy. Luggage had high expectations of privacy.[58] But other containers did not "deserve the full protection of the Fourth Amendment."[59] The bankruptcy of an analytical structure based on

---

a forced surgical procedure to remove a bullet from a person's chest. *See* Winston v. Lee, 470 U.S. 753, 755 (1985). Moreover, even in the area of free speech, the Court has held that a warrant based on probable cause is sufficient authority to search newspaper offices for evidence of a crime. *See* Zurcher v. Stanford Daily, 436 U.S. 547, 566-67 (1978). Congress, in response to *Zurcher*, has imposed several statutory obligations on law enforcement when there is reason to believe that First Amendment materials are involved. *See, e.g.*, CCIPS Manual, *supra* note 46, at 44-47 (discussing the Privacy Protection Act).

[57] Winick, *supra* note 18, at 105.

[58] *See, e.g.*, United States v. Chadwick, 433 U.S. 1, 12-13 (1977) (contrasting reduced expectation of privacy surrounding an automobile with luggage and asserting: "Unlike an automobile, whose primary function is transportation, luggage is intended as a repository of personal effects. In sum, a person's expectations of privacy in personal luggage are substantially greater than in an automobile."); *accord* Florida v. Jimeno, 500 U.S. 248, 253-54 (1991) (Marshall, J., dissenting); *see also* Donald A. Dripps, *The Fourth Amendment and the Fallacy of Composition: Determinacy Versus Legitimacy in a Regime of Bright-Line Rules*, 74 MISS. L.J. 341, 379-87 (2004) (discussing the Court's inconsistent treatment of containers in vehicles).

[59] Arkansas v. Sanders, 442 U.S. 753, 765 n.13 (1979). Indeed, "some containers (for example a kit of burglar tools or a gun case) by their very nature [could not] support any reasonable expectation of privacy because their contents [could]

distinguishing between types of containers soon became evident, at least to a plurality of the Court: it had no basis in the language of the Amendment, which "protects people and their effects, . . . whether they are 'personal' or 'impersonal.'"[60] Thus, the contents of closed footlockers or suitcases and opaque containers were immune from a warrantless search because the owners "reasonably 'manifested an expectation that the contents would remain free from public examination.'"[61] Moreover, the plurality believed that it would be "difficult if not impossible to perceive any objective criteria" to make any distinction between containers: "What one person may put into a suitcase, another may put into a paper bag."[62] A majority of the Court later adopted the view that there was no distinction between "worthy" and "unworthy" containers:

> the central purpose of the Fourth Amendment forecloses such a distinction. For just as the most frail cottage in the kingdom is absolutely entitled to the same guarantees of privacy as the most majestic mansion, so also may a traveler who carries a toothbrush and a few articles of clothing in a paper bag or knotted scarf claim an equal right to conceal his possessions from official inspection as the sophisticated executive with the locked attache case.[63]

Based on this reasoning, it seems clear that the Supreme Court would–and should–reject a special rule for electronic evidence containers. Otherwise, contrary to Supreme Court precedent and sound reasoning, filing cabinets, diaries, books,

---

be inferred from their outward appearance." *Id.*; *accord* Walter v. United States, 447 U.S. 649, 658 n.12 (1980).

[60] Robbins v. California, 453 U.S. 420, 426 (1981) (plurality opinion).

[61] *Id.*

[62] *Id.*

[63] United States v. Ross, 456 U.S. 798, 822 (1982) (footnote omitted); *accord* Florida v. Jimeno, 500 U.S. 248, 253-54 (1991) (Marshall, J., dissenting); *see also* California v. Carney, 471 U.S. 386, 394 (1985) (rejecting distinction between worthy and unworthy motor vehicles); New Jersey v. T.L.O., 469 U.S. 325, 337-39 (1985) (student has protected privacy interest in her purse at school). *But cf.* California v. Greenwood, 486 U.S. 35, 40-41 (1988) (person leaving plastic trash bags for collection has no reasonable expectation of privacy as to the contents of the bags).

floppy drives, hard drives, paper bags, and other storage devices would all require different rules. Moreover, given the pace of technological change, which permits ever greater storage of information on ever smaller devices, such distinctions are illusory. Finally, the fact that some of the evidence in electronic storage is intermingled with other materials should not change the analysis. The same can be said of many other containers: diaries may contain evidence unrelated to the crime; filing cabinets often hold not only files of business-related paper but also miscellaneous other documents, ranging from personal tax records to family photographs.

#### *d. Limitations Based on Search Execution Procedures in Warrants*

Based at least in part on the other premises of the "special approach," that is, computers are different than other containers, that there should be limitations on how the government may conduct a search based on file names or types, or that software search technology must be employed, some authorities require that the warrant set forth the police strategy for executing the search for electronic evidence.[64] Frankly, there is no basis in the language of the Fourth Amendment or Supreme Court caselaw[65] for such warrant requirements. As emphasized by the Supreme Court in *Dalia v. United States,*[66] the Warrant Clause contains three requirements for a search warrant to issue: an oath or affirmation; probable cause to search; and a particular description of the place to be searched.[67] Grounded in that language, the *Dalia* Court rejected the claim that a warrant must specifically authorize a covert entry in order for such a manner of execution of a warrant to be legal. The Court reasoned:

---

[64] *See, e.g., In re* Search of 3817 W. West End, 321 F. Supp. 2d at 958-63 (discussing the particularity requirements as applied to computer searches). The United States Department of Justice's manual on how to search computers may be partly to blame for this because it states that a computer search warrant should set forth a search strategy and the reasons for that strategy. *See* CCIPS Manual, *supra* note 46, 69-75. However, it has been noted that the CCIPS manual is not authoritative on what the Fourth Amendment requires and that, although "it may be preferable and advisable to set forth a computer search strategy in a warrant affidavit, failure to do so does not render computer search provisions unduly broad." *Maali M.*, 346 F. Supp. 2d at 1246. Indeed, the CCIPS manual itself recognizes the inherent difficulty of mandating a predetermined search strategy: "Every computer and computer network is different, and subtle differences in hardware, software, operating systems, and systems configuration can alter the search plan dramatically." CCIPS Manual, *supra* note 46, at 39.

[65] In *Andresen*, the Court did assert that, for document searches and telephone conversation seizures, "responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwar-

> Nothing in the language of the Constitution or in this Court's decisions interpreting that language suggests that . . . warrants also must include a specification of the precise manner in which they are to be executed. On the contrary, it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant-subject of course to the general Fourth Amendment protection "against unreasonable searches

---

ranted intrusions upon privacy." 427 U.S. at 482 n.11. Nothing in that language suggests that the manner in which a search is to be conducted was subject to pre-authorization by the judiciary. Also, *Berger v. New York*, 388 U.S. 41 (1967), properly understood, does not support pre-authorization procedures in a warrant beyond what the Warrant Clause requires. In striking down a statute that authorized wiretapping of telephone conversations, the *Berger* Court identified the statute's failures as noncompliance with the Fourth Amendment's particularity requirements of naming the crime that had been or was being committed and specifying the conversations to be searched. *Id.* at 55-60. The Court added that the statute had the vice of failing to place a termination date on the eavesdrop once the conversation targeted had been seized. *Id.* at 59-60. This latter minimization procedure stems not from Warrant Clause requirements regulating the issuance of a warrant but from the nature of reasonableness, the fundamental command of the first clause of the Amendment, which mandates that the scope of an intrusion must be reasonably related to its justification. *See, e.g.,* New Jersey v. T.L.O., 469 U.S. 325, 341 (1985) (noting the twofold inquiry to assess the reasonableness of a search: initial justification for search and the subsequent scope of that search). Nothing in that reasonableness inquiry requires pre-authorization. Primarily in response to *Berger,* Congress created minimization requirements upon law enforcement officers seeking to intercept electronic communications, mandating that attempts be made to limit interceptions to those conversations that are relevant to the criminal activity that they are authorized to investigate. *See* 18 U.S.C. § 2518(5). Those broad prohibitions have significant application to computer-facilitated communications. *See generally* CCIPS Manual, *supra* note 46, at 164-96.

[66] 441 U.S. 238 (1979).

[67] *Id.* at 255.

> and seizures."
>
> . . . .
>
> It would extend the Warrant Clause to the extreme to require that, whenever it is reasonably likely that Fourth Amendment rights may be affected in more than one way, the court must set forth precisely the procedures to be followed by the executing officers. Such an interpretation is unnecessary, as we have held . . . the manner in which a warrant is executed is subject to later judicial review as to its reasonableness.[68]

Indeed, in the computer context, some courts have recognized that a warrant need not specify the methods of recovery of the data or the tests to be performed because "[t]he warrant process is primarily concerned with identifying *what* may be searched or seized–not how–and *whether* there is sufficient cause for the invasion of privacy thus entailed."[69]

## III. SELECTED FOURTH AMENDMENT APPLICABILITY ISSUES

### *A. Expectation of Privacy Analysis*

### 1. In General

A person seeking to challenge the propriety of a governmental search must establish that she has a protected interest, which the Supreme Court measures by ascertaining whether she has a legitimate expectation of privacy that has been invaded by the government.[70] This expectation of privacy inquiry is two pronged: the individual must show that she has a subjective expectation of privacy; and that that subjective expectation of privacy is one that society is prepared to recognize as reasonable.[71] If either prong is missing, no protected interest is established.[72] The application of this doctrine in the computer context is not without critics;[73] nonetheless, it remains the framework to assess a person's ability to challenge the propriety of governmental searches. The following sections discuss the more common situations where the reasonable expectation of privacy analysis has been applied in the computer context.

---

[68] *Id.* at 257-58 (footnote omitted).

[69] United States v. Upham, 168 F.3d 532, 537 (1st Cir. 1999).

[70] Rakas v. Illinois, 439 U.S. 128, 143 (1978). *But see* Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 327-44 (1998) (discussing origins and development of the privacy expectations test and arguing that it inadequately describes the individual's interests protected by the Fourth Amendment).

[71] *See, e.g.*, Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., con-

### 2. The Location of the Computer—In General

Preliminarily, it is important to distinguish between the exterior of the computer (including what is visible on the monitor's screen) and its contents. As to locating a computer, the person seeking to challenge plain view[74] observations made upon observing the computer must establish an expectation of privacy in the place where the computer is stored.[75]

---

curring); California v. Ciraolo, 476 U.S. 207, 214 (1986) (stating that "Justice Harlan made it crystal clear that he was resting on the reality that one who enters a telephone booth is entitled to assume that his conversation is not being intercepted"); Smith v. Maryland, 442 U.S. 735, 740 (1979) (stating that the Harlan test "embraces two discrete questions").

[72] To support this privacy analysis, the Court has created a hierarchy of privacy interests. First, expectations of privacy that "society is 'prepared to recognize as legitimate'" have, at least in theory, the greatest protection. New Jersey v. T.L.O., 469 U.S. 325, 338 (1985) (quoting Hudson v. Palmer, 468 U.S. 517, 526 (1984)). Second, diminished expectations of privacy are more easily invaded. *See id.* at 342 n.8 (discussing the individual suspicion requirement when privacy interests are minimal); *accord* Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 624-25 (1989). Third, subjective expectations of privacy that society is not prepared to recognize as legitimate have no protection. *See, e.g.,* Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978); United States v. Caymen, 404 F.3d 1196, 1200-01 (9th Cir. 2005) (no reasonable expectation of privacy in the contents of computers the person has stolen or obtained by fraud). *See generally* Clancy, *Concept of Reasonableness, supra* note 56, at 1005-13 (discussing the impact of the privacy hierarchy on the Court's reasonableness analysis).

[73] *See, e.g.,* United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999) ("Cyberspace is a nonphysical 'place' and its very structure, a computer and telephone network that connects millions of users, defies traditional Fourth Amendment analysis. So long as the risk-analysis approach of *Katz* remains valid, however, this court is compelled to apply traditional legal principles to this new and continually evolving technology.").

[74] *See* discussion *infra* at 262-64.

[75] *See, e.g.,* United States v. Lyons, 992 F.2d 1029, 1031-32 (10th Cir. 1993)

Thus, for example, when computers are located in a common storage area accessible to hotel employees and tenants, a person does not have a reasonable expectation of privacy in the physical components of that computer.[76] In contrast, homeowners have a reasonable expectation of privacy in their belongings, including computers, in their home.[77] Equally true, however, is the principle that persons with no expectation of privacy in someone else's home or that home's contents cannot challenge the search or seizure of another's computer in that home.[78]

### 3. Data on Work Computers—Governmental Employer

Government employees may have a legitimate expectation of privacy in their offices or parts of their offices.[79] However, office policies, practices, or regulations may reduce that expectation of privacy.[80] In the context of government computers used by employees, the assessment whether an employee has standing to challenge a search is made "'in the context of the employment relation,' after considering what access other employees or the public had to [the employee's] office"[81] and is done on a case-by-case basis.[82]

When the employer has no policy notifying employees that their computer use could be monitored and there is no indica-

---

(no reasonable expectation of privacy in a stolen hard drive); United States v. Poulsen, 41 F.3d 1330, 1337 (9th Cir. 1994) (holding that a person who failed to pay rent had no reasonable expectation of privacy in the contents of storage locker, including computer tapes).

[76] United States v. Nettles, 175 F. Supp. 2d 1089, 1093-94 (N.D. Ill. 2001).

[77] *Guest*, 255 F.3d at 333; *see also* People v. O'Brien, 769 N.Y.S.2d 654, 656 (N.Y. App. Div. 2003) (defendant had reasonable expectation of privacy in computer in his bedroom).

[78] Guest v. Leis, 255 F.3d at 333.

[79] O'Connor v. Ortega, 480 U.S. 709, 716-18 (1987) (plurality opinion).

[80] *Id.* at 717.

[81] Leventhal v. Knapek, 266 F.3d 64, 73 (2d Cir. 2001) (quoting *O'Connor*, 480 U.S. at 717); *cf.* Voyles v. State, 133 S.W.3d 303, 306 (Tex. App. 2004) (teacher had no reasonable expectation of privacy in computer owned by school district that had been placed on teacher's desk in computer laboratory to teach students about computers).

[82] *O'Connor*, 480 U.S. at 718.

tion that the employer directs others to routinely access the employees' computers, the employees' subjective beliefs that their computer files are private may be objectively reasonable.[83] Thus, for example, in *Leventhal v. Knapek*,[84] the court held that Leventhal had a reasonable expectation of privacy in a computer in a private office that he occupied.[85] He had exclusive use of the computer.[86] The agency did not have a general practice of routinely conducting searches of office computers nor had it placed Leventhal on notice that he should have no expectation of privacy in the contents of his office computer.[87] Although agency technical support staff had access to all computers in the agency's offices, their maintenance of the computers was normally announced; the one unannounced visit to Leventhal's computer was only to change the name of a server.[88] Further, although agency "personnel might also need, at times, to search for a document in an unattended computer," those searches were not so frequent, widespread, or extensive as to constitute an atmosphere "'so open to fellow employees or the public that no expectation of privacy is reasonable.'"[89] The *Leventhal* court concluded that the "'[c]onstitutional protection against *unreasonable* searches by the government does not disappear merely because the government has the right to make reasonable intrusions in its capacity as employer.'"[90]

On the other hand, agency policies and notices indicating that computer use is not private or is subject to inspection or audit have routinely served to defeat expectation of privacy claims.[91] For example, a public employee had no reasonable expectation of privacy in the contents of his government computer based on his written acknowledgement of the agency's policy, which prohibited personal use, expressly stated that employees had no privacy rights, and that the employee consented to inspection and audit of the computer.[92]

---

[83] United States v. Slanina, 283 F.3d 670, 676-77 (5th Cir.), *remanded on other grounds*, 537 U.S. 802 (2002), *on appeal after remand*, 359 F.3d 356 (5th Cir. 2004).

[84] 266 F.3d 64 (2d Cir. 2001).

[85] *Id.* at 73.

[86] *Id.*

[87] *Id.* at 74.

[88] *Id.*

[89] *Id.* at 74 (quoting *O'Connor*, 480 U.S. at 718 (plurality opinion)).

[90] *Id.* (quoting *O'Connor*, 480 U.S. at 717-18 (plurality opinion) (emphasis in original)).

[91] *See* United States v. Angevine, 281 F.3d 1130, 1134-35 (10th Cir. 2002)

### 4. Data on Work Computers—Private Employer

A similar analysis has been applied to work computers owned by a private employer. For example, it has been held that there is no reasonable expectation of privacy in a laptop provided by an employer based on the employer's reserving the right to inspect.[93] Also, a person who has no ownership in a

---

(university policies and procedures, which *inter alia* reserved the right to randomly audit Internet use and to monitor individuals suspected of computer misuse, prevented employees from having reasonable expectation of privacy in data downloaded from the Internet and stored on university computers); United States v. Simons, 206 F.3d 392, 398-99 (4th Cir. 2000) (in light of agency's policy that permitted it to "audit, inspect, and/or monitor" employees' use of Internet, employee did not have reasonable expectation of privacy in files he transferred from the Internet or in the hard drive of computer he used); Wasson v. Sonoma Junior Coll. Dist., 4 F. Supp. 2d 893, 905-06 (N.D. Cal. 1997) (no legitimate expectation of privacy in computer files by employee based on school district's policy that reserved right to "access all information stored on district computers"); United States v. Tanksley, 50 M.J. 609, 620 (N-M. Ct. Crim. App. 1999) (stating there is no reasonable expectation of privacy by military officer in office computer made available to him to perform official duties); United States v. Monroe, 52 M.J. 326, 330 (C.A.A.F. 2000) (no reasonable expectation of privacy in email messages and email box when government-owned email system had banner warning that user of system consented to monitoring); *cf.* Bohach v. Reno, 932 F. Supp. 1232, 1234-35 (D. Nev. 1996) (stating that there is no reasonable expectation of privacy in messages sent over computerized police paging system designed for official communications when all messages were recorded, and notice was given that all messages would be "logged on the network," and that certain messages were banned). *But see* United States v. Long, 61 M.J. 540, 545-47 (N-M. Ct. Crim. App. 2005) (despite banner warning user of possible monitoring of computer network system, the defendant had reasonable expectation in privacy of email on her computer because the system administrator discovered the evidence as a result of a request by law enforcement to locate evidence rather than as a result of routine monitoring).

[92] *Thorn*, 375 F.3d at 683.

[93] Muick v. Glenayre Elec., 280 F.3d 741, 743 (7th Cir. 2002). *Cf.* United States v. Bailey, 272 F. Supp. 2d 822, 824, 835-37 (D. Neb. 2003) (there was no reasonable expectation of privacy in work computer owned by employee's company when company required employee to assent to search every time employee ac-

computer that has been assigned by a company to another user has no standing to challenge its search.[94]

### 5. Information Obtained from Third Parties

If a third party discloses information to the government that an individual has provided to that third party, the individual typically will not have an interest protected by the Fourth Amendment.[95] This is based on the Court's view that no Fourth Amendment protection exists where a wrongdoer has a misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.[96] Such a "risk," according to the Court, is "probably inherent in the conditions of human society."[97] This is consistent with the Supreme Court's view that voluntary exposure to the public eliminates Fourth

---

cessed computer).

[94] United States v. Triumph Capital Group, Inc., 211 F.R.D. 31, 54 (D. Conn. 2002). *Cf.* United States v. Wong, 334 F.3d 831, 839 (9th Cir. 2003) (defendant had no standing to challenge search of former employer's laptop computer).

[95] *See, e.g.,* Miller v. United States, 425 U.S. 435, 443 (1976) (stating rule); United States v. Horowitz, 806 F.2d 1222, 1225-26 (4th Cir. 1986) (no reasonable expectation of privacy in computer data sold to and stored on another company's computer). There is a burgeoning amount of information held by third parties and used by law enforcement. *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1089-1101 (2002) (cataloguing this development). Numerous commentators have argued for Fourth Amendment protections extending to information held by third parties. *See, e.g,* Patricia I. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1403-12 (2004) (arguing that there is a reasonable expectation of privacy in communications held by Internet service providers). Some, as has Professor LaFave, distinguish between the type of information given to the third party and the purposes for which the third party has been given the information and conclude that a person may retain a reasonable expectation of privacy in some circumstances. WAYNE R. LAFAVE, SEARCH AND SEIZURE § 2.6(f) at 717-19 (4th ed. 2004). There is a recent case, which is perhaps a mere aberration, that indicates that the Court may adopt a similar analysis. *See* Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001) (finding a reasonable expectation of privacy by a patient in information conveyed to medical personnel and stating: "The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent.").

[96] Hoffa v. United States, 385 U.S. 293, 302 (1966).

[97] *Id.* at 303.

Amendment protection.[98]

Thus, there is no Fourth Amendment protection[99] against the disclosure of subscriber information by Internet service providers.[100] This rule also applies to email recovered from a third party: once an email message has been received by another party, the sender has no reasonable expectation of privacy in its contents.[101] This risk of exposure analysis also has been uniformly applied to statements made in Internet chat rooms.[102] As one court has stated: "Clearly, when Defendant engaged in chat room conversations, he ran the risk of speaking with an undercover agent."[103]

---

[98] *Katz*, 389 U.S. at 351.

[99] Congress has provided some statutory protections for stored communications in the control of third parties. *See, e.g.*, Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004). Similarly, the interception of communications in transit is largely governed by a statutory framework. *See, e.g.*, Bellia, *supra* note 95, at 1383-96 (outlining the constitutional and statutory framework).

[100] *See* Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (noting that "computer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person—the system operator"); United States v. Cox, 190 F. Supp. 2d 330, 332 (N.D.N.Y. 2002) (holding that there is no reasonable expectation in subscriber information provided to Internet service provider); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (no reasonable expectation of privacy in subscriber information); United States v. Hambrick, 55 F. Supp. 2d 504, 507-09 (W.D. Va. 1999) (individual has no reasonable expectation of privacy in his name, address, social security number, credit card number, screen name, and proof of Internet connection obtained from Internet service provider); State v. Evers, 815 A.2d 432, 440-41 (N.J. 2003) (person had no standing to challenge warrant that obtained his subscriber information from Internet service provider); Hause v. Commonwealth, 83 S.W.3d 1, 10-12 (Ky. App. 2001) (no standing of subscriber to challenge warrant that obtained his name, address, and screen name from Internet service provider); United States v. Ohnesorge, 60 M.J. 946, 949-50 (N-M. Ct. Crim. App. 2005) (no reasonable expectation of privacy in subscriber information given to Internet service provider).

[101] *See, e.g.*, United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997) ("an e-mail message, like a letter, cannot be afforded a reasonable expectation of privacy once that message is received"); United States v. Maxwell, 45 M.J. 406, 418-19 (C.A.A.F. 1996) (no reasonable expectation of privacy in emails after being received by another person); Commonwealth v. Proetto, 771 A.2d 823, 831 (Pa. Super. 2001) (no reasonable expectation of privacy in email messages sent to another person when that person forwarded email to police). *Cf.* United States v. Bach, 310 F.3d 1063, 1066 (8th Cir. 2002) (expressing doubt but declining to decide whether there was a reasonable expectation of privacy in email recovered from Internet service provider).

[102] *See, e.g.*, Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) (no expectation of privacy in material posted on bulletin board system that had disclaimer that

### 6. Joint Users; Password Protected Files

The question also arises where there are joint users of a computer.[104] By creating password-protected files, the creator "affirmatively" intends to exclude the joint user and others from the files.[105] Under such circumstances, it has been reasoned, it cannot be said that the person has assumed the risk that the joint user would permit others to search the files.[106] On the other hand, for example, stating that there is "no generic expectation of privacy for shared usage on computers," one court has held that a student has no standing to suppress session logs, indicating when he used a computer, and evidence on hard drives of the university-owned computer that he used in a computer lab on campus.[107]

---

personal communications were not private); State v. Evers, 815 A.2d 432, 439-40 (N.J. 2003) (person had no reasonable expectation of privacy in "pornographic material he unloosed into the electronic stream of commerce when he e-mailed two photographs . . . to fifty-one chat-room subscribers"); Commonwealth v. Proetto, 771 A.2d 823, 831 (Pa. Super. 2001) (no reasonable expectation of privacy by suspect in his chat-room conversations). *Cf.* United States v. Meek, 366 F.3d 705, 712 n.7 (9th Cir. 2004) (chat room participant had no standing to assert privacy interest of minor's online identity).

[103] United States v. Charbonneau, 979 F. Supp. 1177, 1185 (S.D. Ohio 1997) (no expectation of privacy in statements made in public chat room).

[104] *Cf.* United States v. Longo, 70 F. Supp. 2d 225, 256 (W.D.N.Y. 1999) (no reasonable expectation of privacy by lawyer in computer files accessed by employee in her status as legal secretary).

[105] Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001).

[106] *Id.*; *see also* United States v. Slanina, 283 F.3d 670, 676 (5th Cir.), *remanded on other grounds*, 537 U.S. 802 (2002), *on appeal after remand*, 359 F.3d 356 (5th Cir. 2004) (use of passwords and locking office doors to restrict employer's access to computer files is evidence of employee's subjective expectation of privacy in those files).

[107] United States v. Butler, 151 F. Supp. 2d 82, 84-85 (D. Me. 2001).

### *B. Private Searches and Seizures*

#### 1. In General

The Fourth Amendment is applicable only to governmental activity; hence, private searches and seizures are unregulated by it.[108] Caselaw has detailed three aspects of the private search doctrine that have significance when applied to searches of computers. They are: 1) determining who is a government agent; 2) ascertaining what constitutes replication of a private search; and 3) determining under what circumstances the "context" of a private search destroys any reasonable expectation of privacy in objects not searched by the private party. These latter two questions have been treated by the courts as analytically related and will, therefore, be treated together in this article.

#### 2. Government Agents

The first difficulty is assessing when a person acts as a governmental agent. The Supreme Court has stated that the question whether a person is acting as an agent of the government "necessarily turns on the degree of the Government's participation in the private party's activities, [which] can only be resolved 'in light of all of the circumstances.'"[109] Nonetheless, two considerations for determining when a private party is a government agent are often the focus of the inquiry used by lower courts: (1) whether the government knew or acquiesced in the private party's conduct; and (2) whether the private party's purpose was to assist law enforcement efforts or to further his or her own ends.[110]

---

[108] *See, e.g.,* United States v. Jacobsen, 466 U.S. 109, 113 (1984) (The Fourth Amendment is "wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any government official.'").

[109] Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 614-15 (1989) (citation omitted); *see also* Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971) (a private search may be converted into state action if the private actor is "regarded as having acted as an 'instrument' or agent of the state").

[110] *See, e.g.,* United States v. Soderstrand, 412 F.3d 1146, 1153 (10th Cir.

Although a variety of factual instances have been litigated,[111] a common situation involves repairmen who report their findings to the police. Courts have consistently held that observations by private computer technicians made during their examination of a computer given to them to repair do not implicate the Fourth Amendment.[112] For example, in *United States v. Grimes*,[113] a repairman, during the course of his examination of a computer brought to the computer store for repair by Grimes' wife, opened 17 files that he believed contained child pornography.[114] After consultations with his su-

---

2005); United States v. Steiger, 318 F.3d 1039, 1045 (11th Cir. 2003); United States v. Grimes, 244 F.3d 375, 383 (5th Cir. 2001); Jarrett v. Commonwealth, 594 S.E.2d 295, 300-01 (Va. App. 2004); *see also* United States v. Jarrett, 338 F.3d 339, 344-45 (4th Cir. 2003) (viewing the two parts not as a "test" but as "factors"), *cert. denied*, 540 U.S. 1185 (2004).

[111] *See, e.g.,* United States v. Ellyson, 326 F.3d 522 (4th Cir. 2003) (woman living in defendant's house was not government agent when she turned over to government computer disks containing child pornography); United States v. Poulsen, 41 F.3d 1330, 1335 (9th Cir. 1994) (manager of self-storage unit not acting as government agent when he entered defendant's unit and seized, *inter alia*, computer tapes); United States v. Nettles, 175 F. Supp. 2d 1089, 1091-92 (N.D. Ill. 2001) (Fourth Amendment inapplicable to hotel clerk's moving of computer equipment from hotel room to common storage area when actions were not at behest of government agents); United States v. Longo, 70 F. Supp. 2d 225, 258-60 (W.D.N.Y. 1999) (legal secretary's observations of defendant's computer files were within scope of employment and not a search); State v. Lasaga, 848 A.2d 1149 (Conn. 2004) (private university employee responsible for monitoring computer use not acting as government agent when he detected child pornography on school computer).

[112] *See, e.g.,* United States v. Hall, 142 F.3d 988, 993 (7th Cir. 1998); United States v. Barth, 26 F. Supp. 2d 929, 932-35 (W.D. Tex. 1998) (Fourth Amendment inapplicable to computer repairman's examination of computer when performing repair work); People v. Phillips, 831 N.E.2d 574, 582 (Ill. 2005) (no search when police shown child pornography video on computer that had been previously viewed by computer repairman during course of repair efforts); People v. Emerson, 766 N.Y.S.2d 482, 486-87 (N.Y. Sup. Ct. 2003) (no reasonable expectation of privacy and hence, no search, when private computer repairman showed child pornography computer files to police that he had previously viewed). *Cf.* Rogers v. State, 113 S.W.3d 452, 457-48 (Tex. App. 2003) (finding no reasonable expectation of privacy in computer files that defendant had requested computer repairman to copy).

[113] 244 F.3d 375 (5th Cir. 2001).

[114] *Grimes*, 244 F.3d at 377-83.

pervisor, the technician called the police.[115] An officer then came to the store and viewed the same 17 images.[116] Without requesting the store employees to search the computer any further, the officer reported the findings to a FBI agent.[117] The repairman's supervisor, meanwhile, copied the 17 images onto a floppy disk, which he gave to the police officer; the officer copied them before faxing the images to the FBI agent, who later seized the computer after obtaining a search warrant.[118] Grimes claimed that the store's search went beyond the permission given by his wife, thereby invalidating any evidence that flowed from the search.[119] The court found that the initial search, being private in nature, was not subject to Fourth Amendment applicability.[120] It reasoned that the government was not involved in the discovery of the 17 images nor were the private parties acting with the intent to assist law enforcement officials.[121] The court believed that the pre-warrant images viewed by the police officer and the FBI agent were "within the scope of the original private-party search" and "were in an area where Grimes no longer possessed a reasonable expectation of privacy."[122]

On the other hand, it has been held, when a repairman copied files based on a state trooper's request, a search within the meaning of the Amendment occurred.[123] Similarly, although a private computer repairman was acting in a private capacity when he observed the first file containing child pornography, after he related his observations to a FBI agent who asked him to copy the entire hard drive, his observations of additional files were as a government agent.[124]

---

[115] *Id.* at 378.
[116] *Id.*
[117] *Id.*
[118] *Id.*
[119] *Id.* at 383.
[120] *Id.*
[121] *Id.*
[122] *Id.*
[123] United States v. Hall, 142 F.3d 988, 993 (7th Cir. 1998); *see also* United States v. Barth, 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998) (computer repairman's first viewing of child pornography not a search but his later viewing of additional files after reporting his observation to police was as government agent).

Other common searches involve hackers.[125] An anonymous computer hacker, known as "Unknownuser," has generated several prosecutions for possession of child pornography stemming from his hacking activities.[126] Unknownuser obtained access to the computers via a Trojan horse program that he attached to a picture he posted to a news group frequented by persons interested in pornography. When the picture was downloaded, the Trojan horse program was also downloaded, allowing Unknownuser to gain access to the computers.[127] After finding child pornography, Unknownuser reported those findings to law enforcement authorities.

Although Unknownuser was truly unknown to law enforcement prior to his first report, thus making the conclusion that he was not a government agent an easy one,[128] Unknownuser's subsequent efforts were preceded by an FBI agent's thanking him for his assistance in the first case and by the comment: "If you want to bring other information forward, I am available."[129] Several months later, Unknownuser produced information about another child molester.[130] Two different appellate courts subsequently rejected the claim that Unknownuser acted as a government agent based on the FBI agent's comments, reasoning that, although Unknownuser was motivated to aid law enforcement, the government did not involve itself in Unknownuser's search sufficiently to transform it into governmental action.[131] Those courts asserted that mere acquiescence was insufficient; rather, the government must either participate in or affirmatively encourage the search.[132] The mere expression of gratitude did not create an agency relationship; otherwise, as one court stated, "virtually any Government expression of gratitude for assistance well prior to an investigation would effectively transform any subsequent private search by the party into a Government search."[133] The court noted that the government was under no affirmative obligation to discourage Unknownuser from hacking.[134]

---

[124] *Barth*, 26 F. Supp. 2d at 935-36. *But see* United States v. Peterson, 294 F. Supp. 2d 797, 800, 805 (D.S.C. 2003) (technician's observation of child pornography during repair of computer was not as agent of government, despite South Carolina statute requiring technician to report such observations and despite the fact that, after the technician's initial observations, he decided to open additional files because of that legal requirement).

[125] *See* Monica R. Shah, Note, *The Case for a Statutory Suppression Remedy to Regulate Illegal Private Party Searches,* 105 COLUM. L. REV. 250 (2005) (discussing ability of private citizens to hack into computers of other persons).

[126] *See* United States v. Jarrett, 338 F.3d 339 (4th Cir. 2003); United States v. Steiger, 318 F.3d 1039, 1042-46 (11th Cir. 2003) (no search when private hacker turned child pornography over to police that hacker found by accessing defendant's computer); Jarrett v. Commonwealth, 594 S.E.2d 295, 301-03 (Va. App. 2004) (same).

[127] *Jarrett*, 338 F.3d at 341.

[128] *Steiger*, 318 F.3d at 1045.

[129] *Jarrett*, 338 F.3d at 341.

[130] *Id.* at 342.

Subsequent to Unknownuser's providing the information that formed the basis of the second and third prosecutions, an FBI agent began a series of e-mail exchanges with Unknownuser, which one appellate court has described as the "proverbial 'wink and a nod.'"[135] The agent informed Unknownuser that she could not ask him to search for additional child pornographers because that would make him an agent of the government and make the information he obtained unuseable.[136] The agent further advised that Unknownuser should feel free to send any additional information he obtained and that he would not be prosecuted for hacking.[137] The Fourth Circuit viewed those exchanges as "probably" the type of government involvement that would create an agency relationship.[138]

---

[131] *Id.* at 345; *Jarrett*, 594 S.E.2d at 302-03.

[132] *Jarrett*, 338 F.3d at 345.

[133] *Id.* at 346.

[134] *Id.* at 347.

[135] *Id.* at 343.

[136] *Id.*

[137] *Id.*

[138] *Id.* at 346.

### 3. Replication and "Context" Issues

A government search that merely replicates a previous private one is not a "search" within the meaning of the Fourth Amendment; rather, the Amendment applies only to the extent that the government has exceeded the scope of the private search.[139] The reasoning behind this rule, generally speaking, is that the original private party search extinguishes any reasonable expectation of privacy in the object searched.[140] The application of these principles in the computer context has sometimes led to questionable results. For example, although a computer repairman detained a computer for an extra day based on the FBI's request to do so to allow time for the FBI to obtain a search warrant, one court maintained that the detention was not attributable to the government.[141]

There are also situations where the "context" in which an object is found may lead some courts to the conclusion that there is no legitimate expectation of privacy in that object.[142] According to this view, due to the private search, there may not be any legitimate expectation of privacy remaining in aspects of the object that had not been examined during that private search. Under such circumstances, it might be concluded that the government expansion of the private intrusion does not invade any protected interest, which is to say that there is no search within the meaning of the Fourth Amendment. Frankly, the caselaw is less than clear whether this principle is firmly established–at least in Supreme Court jurisprudence.

The analysis of these principles begins with *Walter v. Unit-*

---

[139] United States v. Jacobsen, 466 U.S. 109, 115 (1984).

[140] *Id.* at 120-21.

[141] United States v. Hall, 142 F.3d 988, 994-95 (7th Cir. 1998).

[142] *See, e.g., Jacobsen*, 466 U.S. at 121 (although private party had not physically examined contents of package containing white powder, package could no longer support reasonable expectation of privacy); *id.* at 143 (Brennan, J., dissenting) (observing that the "context in which the white powder was found" under his view of the facts "could not support a reasonable expectation of privacy" and that there was a "'virtual certainty'" that the DEA agent could identify it). *Cf.* Texas v. Brown, 460 U.S. 730, 743 (1983) (plurality opinion) (balloon had "distinctive character [that] spoke volumes as to its content–particularly to the trained eye of the officer").

*ed States*.[143] In that case, 12 packages were delivered to the wrong company.[144] Employees opened the packages; inside the packages were 871 boxes of 8-millimeter film.[145] On one side of each box "were suggestive drawings, and on the other were explicit descriptions of the contents."[146] One employee attempted to hold one or two of the films up to the light, but was unable to observe the content of the films.[147] The recipients contacted federal agents, who viewed the films with a projector without first obtaining a warrant to search.

---

[143] 447 U.S. 649 (1980).

[144] *Id.* at 651.

[145] *Id.* at 652.

[146] *Id.* The Supreme Court did not detail the information on the boxes. The lower court, however, stated that "[t]he top of each film box showed the name 'David's Boys' and a drawing of two nude males embracing and kissing; on the back of each were the title of the individual movie and a detailed description, in explicit terms, of the bizarre homosexual acts depicted in the film." United States v. Sanders, 592 F.2d 788, 791 (5th Cir. 1979). The court detailed:

> The indictment listed five of the 25 "David's Boys" titles included in the shipment. The individual boxes containing "Look at the Birdie" said that Corbett really gets turned on when Rich comes over for a photo session. In the a—close-ups you won't believe ! The highlight of the movie happens when Corbett masturbates and—on Rich's face! This is a flick you will not forget.
>
> "The Clean Up (3 white)" boxes read that Lenny and Eric turn each other on and when you see these good looking studs you'll know why! ! ! The action gets heavy and then Les enters the picture. galore and Les cleans it up like you've never seen. Great close-ups!
>
> The "Black Rape" (1 blk. 1 wht.) boxes stated that Big Black Lance as 11—but it doesn't take long before the small slender Larry is taking it all right up the ! Good tongue action and a surprise that you won't believe. You will love the close-up action. The boxes containing "The Massage" explained that Angelo the masseur gets turned on as he gives Tommy a rubdown. Angelo's expert tongue & hands soon have Tommy's hard & excited. But he wants it the Greek way and Angie complies. Then he beautiful on Tommy's face! This is one of the best close-ups of french love you will ever see! !
>
> Finally, the "Loving Hands" boxes said that Murray and Carl are well into their love session when Ben enters the room. He will show you his loving hands as he shoves them with his arms (just short of his elbows!) right up his friends' ah ! ! While they masturbate! It is a true masterpiece for the avid connoisseur! ! (Certain particularly salacious words have been deleted by the writer of this opinion, as indicated.)

*Id.* at 793 n.5.

[147] *Walter,* 447 U.S. at 651.

Although a majority of the Court concluded that the viewing of the films using a projector violated the Fourth Amendment, there was no majority opinion. In an opinion announcing the judgment of the Court, authored by Justice Stevens and joined by only one other Justice, Stevens asserted that the officers violated the Fourth Amendment because they exceeded the scope of the private search.[148] He reasoned that, because the private party had not actually viewed the films, projecting "the films was a significant expansion of the search that had been conducted previously by a private party and therefore must be characterized as a separate search."[149] This was despite the fact that "the nature of the contents of these films was indicated by descriptive material on their individual containers."[150] Stevens maintained:

> [T]he labels on the film boxes gave [the federal agents] probable cause to believe that the films were obscene and that their shipment in interstate commerce had offended the federal criminal code. But the labels were not sufficient to support a conviction and were not mentioned in the indictment. Further investigation–that is to say, a search of the contents of the films–was necessary in order to obtain the evidence which was to be used at trial.[151]

Stevens rejected the government's claim "that because the packages had been opened by a private party, thereby exposing the descriptive labels on the boxes, petitioners no longer had any reasonable expectation of privacy in the films."[152] He believed that "[t]he private search merely frustrated that expectation in part. It did not simply strip the remaining unfrustrated portion of that expectation of all Fourth Amendment protection."[153] In a curious footnote, however, Justice Stevens opined that "if a gun case is delivered to a carrier, there could then be no expectation that the contents would remain private, but if the gun case were enclosed in a locked suitcase, the shipper would surely expect that the privacy of its contents would be respected."[154] The gun case example indicates that Stevens would hold that, in at least some circumstances where the objects inside the container can be ascertained by information outside the container, there is no reasonable expectation of privacy inside the container. Stevens, however, made no attempt to reconcile the gun case example with the facts or his analysis in *Walter*.[155]

---

[148] *Id.* at 657. Justice White, in a concurring opinion joined by Justice Brennan, believed the Fourth Amendment was violated because the agents had not obtained a warrant, regardless of whether the scope of the private search was exceeded. *Id.* at 660-62. Justice Marshall concurred in the judgment but did not write an opinion. *Id.* at 660.

[149] *Id.* at 657.

[150] *Id.* at 654.

[151] *Id.*

[152] *Id.* at 658.

The four dissenters in *Walter* believed that no legitimate expectation of privacy remained in the contents of the packages by the time the FBI received them because the private search had "clearly revealed the nature of their contents."[156] Accordingly, the viewing of the films by the FBI did not change the nature of the search and was not an additional search.[157] The dissent also addressed Stevens' gun case hypothetical: "The films in question were in a state no different from Mr. Justice Stevens' hypothetical gun case when they reached the FBI. Their contents were obvious from 'the condition of the package,' . . . and those contents had been exposed as a result of a purely private search that did not implicate the Fourth Amendment."[158]

A perplexing question involving searches of computers, which has led to contradictory results, involves whether the scope of the private party search has been exceeded when law enforcement agents open additional files that had not been opened in the preceding private search. This question is similar to the one that so divided the Court in *Walter*. Some courts have held that the determinative inquiry is not the mere opening of additional files.[159] On the other hand, in *United States v. Barth*,[160] the court rejected the government's contention that, once a private computer repairman opened a file containing an image of child pornography, Barth lost his reasonable expectation of privacy in the other files on the computer's hard drive, reasoning that the copying of the entire contents of the hard drive and the review of those files by law enforcement "far exceeded" the private viewings.[161]

---

[153] *Id.* at 659.

[154] *Id.* at 658 n.12 (citation omitted).

[155] The gun case has been repeated several times to illustrate the situation where the "very nature" of the container "cannot support any reasonable expectation of privacy because [the] contents can be inferred from [the] outward appearance." Arkansas v. Sanders, 442 U.S. 753, 764-65 n.13 (1979); *see also Jacobsen*, 466 U.S. at 121 (repeating the gun case example).

[156] *Walter*, 447 U.S. at 663 (Blackmun, J. dissenting).

[157] *Id.* at 663-64 (citation omitted).

[158] *Id.* at 665.

In this context, *United States v. Runyan*[162] is particularly instructive. In that case, the defendant's estranged wife and her companions removed from Runyan's ranch various data storage devices and turned them over to the police. The private parties had examined only a randomly selected assortment of the floppy disks and CDs and they did not view any of the ZIP disks. The government agents examined every one of the floppy disks, ZIP disks, and CDs.[163]

The *Runyan* court noted that there are two different analytical approaches to the problem posed by the facts. One line of authority holds that "a police search exceeds the scope of a prior private search when the police open a container that the private searchers did not open."[164] A second line, according to the court, is reflected in *United States v. Bowman*:[165]

---

[159] *See, e.g.*, People v. Emerson, 766 N.Y.S.2d 482, 488 (N.Y. Sup. Ct. 2003) ("when an earlier, private search opens child pornography images on a hard drive in identified computer file folders which the private searcher found replete with file titles plainly suggesting images of like kind, defendant retains no reasonable expectation of privacy with respect to additional such image files in the same two computer file folders"). *Cf.* State v. Lasaga, 848 A.2d 1149 (Conn. 2004) (declining to determine if police exceeded scope of private search when they opened additional files because, even if those files were disregarded, warrant based on probable cause to search).

[160] 26 F. Supp. 2d 929 (W.D. Tex. 1998).

[161] *Id.* at 935-37.

[162] 275 F.3d 449, 453-57 (5th Cir. 2001).

[163] *Id.* at 461-62.

[164] *Id.* at 462.

> In *Bowman,* an airline employee opened an unclaimed suitcase and found five identical bundles wrapped in towels and clothing The employee opened one bundle and found a white powdery substance wrapped in plastic and duct tape. He contacted a federal narcotics agent, who identified the exposed bundle as a kilo brick of cocaine and then opened the other bundles, which also contained kilo bricks of cocaine. The court held that the agent did not act improperly in failing to secure a warrant to unwrap the remaining identical bundles, reasoning that the presence of the cocaine in the exposed bundle "'spoke volumes as to [the] contents [of the remaining bundles]—particularly to the trained eye of the officer.'"[166]

*Runyan* attempted to harmonize the two approaches:

> [C]onfirmation of prior knowledge does not constitute exceeding the scope of a private search. In the context of a search involving a number of closed containers, this suggests that opening a container that was not opened by private searchers would not necessarily be problematic if the police knew with substantial certainty, based on the statements of the private searchers, their replication of the private search, and their expertise, what they would find inside. Such an "expansion" of the private search provides the police with no additional knowledge that they did not already obtain from the underlying private search and frustrates no expectation of privacy that has not already been frustrated.[167]

Applying this guideline to the facts of the case before it, the *Runyan* court believed that the police's pre-warrant examination of the disks not opened by the private parties clearly exceeded the scope of the private search:

> The police could not have concluded with substantial certainty that all of the disks contained child pornography based on knowledge obtained from the private searchers, information

---

[165] 907 F.2d 63 (8th Cir. 1990).

[166] 275 F.3d at 462-63 (quoting *Bowman*, 907 F.2d at 65).

[167] *Id.* at 463 (citations omitted).

> in plain view, or their own expertise. There was nothing on the outside of any disk indicating its contents. . . . Indeed, [the private searchers] could not have known the contents of any of the ZIP disks, as [they] did not use hardware capable of reading these disks in their private search. The mere fact that the disks that [the private searchers] did not examine were found in the same location in Runyan's residence as the disks they did examine is insufficient to establish with substantial certainty that all of the storage media in question contained child pornography.[168]

Turning to the question whether the police exceeded the scope of the private search because they opened more files on each of the disks than examined by the private searchers, while the record was not entirely clear whether the police actually did so, the court concluded that it would not have been constitutionally problematic for the police to have examined more files than did the private searchers.[169] The court reasoned:

> [T]he police do not exceed the scope of a prior private search when they examine the same materials that were examined by the private searchers, but they examine these materials more thoroughly than did the private parties. In the context of a closed container search, this means that the police do not exceed the private search when they examine more items within a closed container than did the private searchers. . . . [A]n individual's expectation of privacy in the contents of a container has already been compromised if that container was opened and examined by private searchers[.] Thus, the police do not engage in a new "search" for Fourth Amendment purposes each time they examine a particular item found within the container.[170]

*Runyan's* approach is open to criticism. One can take issue with the court's view of what the appropriate container is: should it be the computer; an individual disk; the directory; the file folders; or each individual file? *Runyan* seems to point to each disk as the container and, hence, once that disk is opened by the private party, anything within it that the police examine is within the scope of the private search. The basis for the court's analysis is far from clear: why is not the entire hard drive of a computer the container and, once that container is opened by a private party, all data would be within that search's scope; on the other hand, why is not each data file a container, given that each must be separately "opened" to view the file's contents?

---

[168] *Id.* at 464.

[169] *Id.*

[170] *Id.* at 464-65.

One could draw an analogy to a filing cabinet in the physical world. Each filing cabinet may have one or more drawers and have a number of file folders in each drawer. For example, there may be a group of folders entitled tax records, each for a different year. If a private party opens "tax records 2004," under *Runyan* it would seem that the tax records for other years may be opened by government agents and not be labeled a search. This approach is undoubtedly incorrect. Nothing in previous Supreme Court caselaw supports viewing the entire filing cabinet as a container that permits wholesale searches of all the files therein once a private party opens one of them.[171] If computers are containers that hold various forms of information,[172] then there is no principled distinction between them and a metal filing cabinet when applying the private search doctrine. This is to say that the rules regulating containers in the bricks and mortar world have equal applicability to computer searches. Accordingly, a computer should be viewed as a physical container with a series of electronic "containers"–that is, directories, folders, and files that must be each separately opened. Each separate opening is the examination of a new container.

Also, to the extent that *Runyan* grounds its analysis on the belief that the mere opening of additional files within a container already partially examined by a private party does not exceed the scope of that private search because the "container" no longer supports a reasonable expectation of privacy, there is little Supreme Court jurisprudence to support that view. Only in *United States v. Jacobsen*[173] has the Supreme Court held that the government activities were not a search, even though the government activity exceeded the private search. In that case, a Federal Express employee opened a damaged package and found several transparent plastic bags of white powder inside a closed tube wrapped in crumpled newspaper. The employee put the bags back in the tube, put the tube and the newspapers back in the box, and then summoned federal agents. The agent who responded opened the box, unpacked the bags of white powder, and performed a chemical field test confirming that the white powder was cocaine.[174] Putting aside the chemical testing, which raised a separate issue,[175] the Court found that the agent's actions did not implicate the Fourth Amendment because the agent's actions in removing the plastic bags from the tube and visually inspecting their contents "enabled the agent to learn nothing that had not previously been learned during the private search."[176] Although the private party had not physically examined the contents of the package containing the white powder, the Court asserted that the package could no longer support a reasonable expectation of privacy.[177] The Court concluded that the visual inspection was not a "search" because it did not infringe "any constitutionally protected privacy interest that had not already been frustrated as the result of private conduct."[178] By merely replicating the private party's actions, the agents in *Jacobsen* observed white powder in a *transparent* container. They learned nothing more from its mere removal, which is to say that no reasonable expectation of privacy was invaded by their actions. This is in marked contrast to *Runyan*, where the container did not disclose its contents prior to its opening and, as a result, the police did learn something new when the files were opened.

---

[171] *Cf.* United States v. Knoll, 16 F.3d 1313, 1321 (2d Cir. 1994) (viewing each closed opaque file folder as closed container).

[172] *See* discussion *supra* at 197-220.

---

[173] 466 U.S. 109 (1984).

[174] *Id.* at 111-12.

[175] *See id.* at 123.

[176] *Id.* at 120.

[177] *Id.* at 121; *see also id.* at 142 (Brennan, J., dissenting) (observing that the "context in which the white powder was found" under his view of the facts "could not support a reasonable expectation of privacy" and that there was a "'virtual certainty'" that the DEA agent could identify it).

[178] *Id.* at 126.

This leaves the difficult decision of *Walter* as possible support for the *Runyan* viewpoint. Clearly, the Court has changed since *Walter* and a majority might be willing to adopt the *Walter* dissent's view that context does sometimes destroy an expectation of privacy, even if the private party had not opened the same container as the governmental authorities. On the other hand, if Justice Stevens' view in *Walter* is adopted by a majority of the Court, it is difficult to envision a situation where the police could open a computer file unopened by the private party without exceeding the scope of that private search. The boxes in *Walter* certainly gave the police a high degree of confidence that they contained pornography.[179] So too would a private party search that opened some files with suggestive names that were in a folder with a series of other files. Thus, for example, if a private party opened files labeled "preteen.female9.rape", "preteen.female10.rape", and preteen.female11.rape," and discovered images of young girls being raped, if there were additional files in the same folder labeled "preteen.female12.rape" and "preteen.female13.rape", I would think that most courts would easily conclude that the police had probable cause to believe that the "12" and "13" files also depicted images of child pornography. But under Stevens' view in *Walter*, mere probable cause–or even "substantial certainty"–does not eliminate Fourth Amendment applicability.

This, it seems to me, is the proper approach. Probable cause is the usual level of suspicion that justifies a search. Moving to a higher level of suspicion, such as "substantial certainty," does not somehow make the Amendment inapplicable. The opposing position would hold that, the more certain the police are, the less applicable the Amendment becomes. That position confuses Fourth Amendment applicability with

---

[179] *See supra* notes 143-47 and accompanying text.

Fourth Amendment satisfaction.[180] Underlying the private search doctrine is the view that the private party has already discovered what is in the container; in the Court's words, the private party has eliminated the owner's reasonable expectation of privacy in the contents of the container. Yet, when the governmental agent opens an opaque container that a private party has not opened, the agent does learn something that the private party did not learn. That is, the container does *in fact* hold a gun, drugs, or child pornography, or that the container *in fact* holds something else – despite all indications of what it held prior to its opening.

Finally, there remains the oft-stated gun case hypothetical. This is much different than the situation in *Jacobsen*, where the contents of the *transparent* package could be viewed without opening the container. The gun case hypothetical envisions a container that is specifically designed to hold a gun and whose exterior shape informs the observer that it is a gun case.[181] However, putting aside transparent gun cases, the shape of the case does not disclose what is inside; instead, it informs the observer that it is a case designed to hold guns and perhaps–or even probably–that there is a gun inside. The police will not *know* what is inside until they open the case or use other means, such as an x-ray, to examine its contents. The dissent in *Walter* was correct in asserting that the viewing of the films in that case and the gun case hypothetical presented identical scenarios. Yet, in both situations, although the police may have had a high degree of confidence in what they would find when they opened the container, that confidence should not eliminate the applicability of the Amendment; instead, that confidence goes to the reasonableness of the police's actions.[182]

---

[180] *Cf.* Soldal v Cook County, 506 U.S. 56, 69 (1992) ("[T]he reason why an officer might enter a house or effectuate a seizure is wholly irrelevant to the threshold question whether the Amendment applies. What matters is the intrusion on the people's security from governmental interference.").

[181] Gun cases come in many forms: some are mere rectangular hard-sided boxes; others are soft-sided and in the shape of a rifle or a shotgun. Rectangular boxes disclose nothing of the contents of the box. Instead, the gun case hypothetical refers to those containers that have the unique shape that says to the viewer that is a container designed to hold a gun.

## IV. SELECTED SATISFACTION ISSUES

### *A. Probable Cause*

The concept of probable cause–a familiar but fluid standard for a court to apply[183]–has created some unique difficulties in the computer context.[184] This article focuses on two nexus questions that have troubled the courts confronting them: 1) as to subscribers of child pornography sites, the amount of information needed in order to conclude that there is probable cause to search the subscriber's computer; and 2) as to distributors or recipients of child pornography, establishing the location of the computer used to distribute or receive the materials.[185] Both of these problems illuminate the difficulty of piercing through the layers of anonymity that the Internet affords.

---

[182] *Cf.* Clancy, *Concept of Reasonableness*, *supra* note 57, at 1000-03 (discussing the Court's inconsistent treatment of containers as to application of warrant preference rule and arguing that there should be no warrant requirement for "effects").

[183] *See generally* Ronald J. Bacigal, *Making the Right Gamble: The Odds on Probable Cause*, 74 MISS. L.J. 279 (2004) (comprehensively examining the concept of probable cause). "In dealing with probable cause . . . as the very name implies, we deal with probabilities. These are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." Brinegar v. United States, 338 U.S. 160, 175 (1949). The totality of the circumstances is taken into account to determine whether there is a "fair probability that contraband or evidence of a crime will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 238 (1983). In reviewing a warrant that had been issued by a magistrate, a court does not make a *de novo* determination of probable cause; instead, the proper question is whether a substantial basis exits for the magistrate's finding of probable cause. *Id.* at 236.

[184] As with other situations, probable cause determinations in the computer context are fact-bound. *See, e.g.,* United States v. Hill, 322 F. Supp. 2d 1081, 1084-87 (C.D. Cal. 2004) (discussing when allegations of child pornography are sufficient); United States v. Scott, 83 F. Supp. 2d 187, 197 (D. Mass. 2000) (it is "reasonable to suppose that someone allegedly engaged in bank fraud and producing false securities on his computer would have records of the bank fraud and false securities on that computer"); Burnett v. State, 848 So. 2d 1170, 1173-75 (Fla. App. 2003) (no probable cause to support warrant to search computer for evidence of child pornography based on initial complaint that suspect had made lewd videotape of two children); State v. Staley, 548 S.E.2d 26, 28-29 (Ga. App. 2001) (although police had probable cause to believe that Staley had molested a specific child, that he had worked as a computer analyst, that he had been previously convicted of molesting a child and taking pictures of that child, and that the affiant detailed that pedophiles stored information relating to having sex with children, there was no nexus between either the crime of molesting that specific child or the propensities of child sex offenders and search of computer in Staley's apartment); State v. Lum, 998 P.2d 137, 139-42 (Kan. Ct. App. 2000) (affidavit in support of search warrant for computer insufficient because affiant failed to detail basis of knowledge); Williford v. State, 127 S.W.3d 309, 313 (Tex. App. 2004) (probable cause to seize computer based on repairman's viewing of thumbnail picture of two naked boys on bed); Burke v. State, 27 S.W.3d 651, 653-56 (Tex.

There is a split of authority over the strength of the inference that can be drawn as to whether a person has child pornography on his computer based on membership in a child pornography web site. A few courts have indicated that mere membership in a child pornography site is sufficient.[186] Oth-

---

App. 2000) (fact-bound question whether there was probable cause to issue warrant in child pornography case).

A persistent question concerns the circumstances under which file names establish probable cause to search or seize a computer; a finding of probable cause generally turns on the explicit nature of the names and the surrounding circumstances. *See, e.g.,* State v. Wible, 51 P.3d 830, 833-34 (Wash. App. 2002) (file names "8 year old Rape" and "8 year old Smile" gave context and meaning to repairman's tip that computer contained child pornography).

[185] The number of child pornographers utilizing the Internet is truly shocking and law enforcement efforts to catch those criminals comprise a large portion of the published decisions dealing with computer-related search and seizures. *See, e.g.,* Amy E. Wells, Comment, *Criminal Procedure: The Fourth Amendment Collides with the Problem of Child Pornography and the Internet*, 53 OKLA. L. REV. 99, 100-01 (2000) (cataloguing reasons for explosion of Internet child pornography). The Internet has increasingly become a preferred vehicle to trade and distribute child pornography; websites are designed for that purpose and chat rooms are used to establish contacts, followed by transmission or trading of images. *See, e.g.,* United States v. Hay, 231 F.3d 630, 636 (9th Cir. 2000). Because of a computer's ability to store images in digital form, it is an ideal repository for child pornography. *Id.* at 635-36.

[186] *See* United States v. Martin, 426 F.3d 3 (2d Cir. 2005) (finding probable cause based on subscription to website that's essential purpose was to trade child pornography); United States v. Wagers, 339 F. Supp. 2d 934 (E.D. Ky. 2004) (probable cause existed that suspect's home computer contained child pornography based on membership in child pornography website); U.S. v. Bailey, 272 F. Supp. 2d 822, 824-25 (D. Neb. 2003) (holding that "knowingly becoming a computer subscriber to a specialized Internet site that frequently, obviously, unquestionably and sometimes automatically distributes electronic images of child pornography to other computer subscribers alone establishes probable cause for a search of the

ers have rejected that view.[187] Those latter courts caution:

> If the Government is correct in its position that membership in the Candyman group [an Internet child pornography site] *alone* was sufficient to support a finding of probable cause, then probable cause existed to intrude into the homes of some 3,400 (or even 6,000) individuals merely because their e-mail addresses were entered into the Candyman website. Without any indication that any of these individuals downloaded or uploaded or transmitted or received any images of child pornography, without any evidence that these individuals did anything more than simply subscribe, the Government argues that it had the right to enter their homes to conduct a search and seize their computers, computer files and equipment, scanners, and digital cameras. This cannot be what the Fourth Amendment contemplated.
>
> * * * * Here, the intrusion is potentially enormous: thousands of individuals would be subject to search, their homes invaded and their property seized, in one fell swoop, even though their only activity consisted of entering an e-mail address into a website from a computer located in the confines of their own homes. In fact, here the FBI sent out 700 or more draft search warrants across the country. . . . In light of the potential impact, care must be taken.[188]

---

target subscriber's computer even though it is conceivable that the person subscribing to the child pornography site did so for innocent purposes and even though there is no direct evidence that the target subscriber actually received child pornography on his or her computer").

[187] *See* United States v. Gourde, 382 F.3d 1003, 1006, 1011-13 (9th Cir. 2004) (holding that merely because suspect was member of Internet child pornography site for at least two months was insufficient to establish that he had downloaded child pornography onto his home computer, despite a discussion of traits of child pornography collectors by affiant that included explanations that they "rarely if ever" dispose of pornography and that they use the Internet to share information and trade child pornography), *reh'g granted*, 416 F.3d 961 (9th Cir. 2005); United States v. Perez, 247 F. Supp. 2d 459, 483-84 (S.D.N.Y. 2003) (subscription to known child pornography website created a "chance, but not a fair probability, that child pornography would be found"). *But see* United States v. Corcas, 419 F.3d 151 (2d Cir. 2005) (although affirming denial of motion to suppress, the panel did so based on prior precedent finding probable cause stemming from membership in child pornography website, while criticizing that precedent as unsound).

[188] *Perez*, 247 F. Supp. 2d at 483-84.

To establish probable cause to search, courts often rely on additional information–beyond membership in a child pornography site–that substantiates the person's sexual interest in children or in child pornography.[189] That additional information has included such factors as evidence of actual downloading[190]–as opposed to mere viewing,[191] automatic transmissions as part of the site's services,[192] use of suggestive screen names,[193] expert information on the retention habits of child pornography collectors[194] (which often serves to dispel

---

[189] *See, e.g.,* United States v. Froman, 355 F.3d 882, 884-91 (5th Cir. 2004) (upholding search warrant for member of group whose "singular goal . . . was to collect and distribute child pornography and sexually explicit images of children," when members could choose to automatically receive emails with attached images and Froman's interest in child pornography was shown by his chosen screen names, "Littlebuttsue" and "Littletitgirly"); State v. Schaefer, 668 N.W.2d 760, 770 (Wis. App. 2003) (because computer files are common way of storing photographs, reasonable inference that computer contained child pornography when suspect actively cultivated friendship of teenage boys by inviting them to use his home computer, used his computer to communicate with others interested in stories about adults sexually assaulting children, and visited Internet sites where child pornography was available for downloading).

[190] *Gourde*, 382 F.3d at 1006, 1012 ("Requiring the government to buttress its affidavit with personalized information linking a website member to actual child pornography strikes a reasonable balance between safeguarding the important Fourth Amendment principles embodied in the probable cause requirement and ensuring that the government can effectively prosecute possessors and distributors of child pornography."); United States v. Perez, 247 F. Supp. 2d 459, 483-84 (S.D.N.Y. 2003) (rejecting finding of probable cause and noting, *inter alia*, that, unlike other cases where there was evidence of downloading, the affidavit contained "nothing concrete to suggest that Perez had transmitted or received images of child pornography").

[191] *See Perez*, 247 F. Supp. 2d at 483-84 n.12 ("The statute does not criminalize 'viewing' the images, and there remains the issue of whether images viewed on the internet and automatically stored in a browser's temporary file cache are knowingly 'possessed' or 'received.'"); *see also* United States v. Zimmerman, 277 F.3d 426, 435 (3d Cir. 2002) (without evidence that pornography was specifically downloaded and saved to defendant's computer, offending images "may well have been located in cyberspace, not in [the defendant's] home"); United States v. Tucker, 305 F.3d 1193, 1198 (10th Cir. 2002) (upholding conviction for possession of files automatically stored in browser cache because defendant's habit of manually deleting images from cache files established his control over them).

[192] *See Perez*, 247 F. Supp. 2d at 485 (asserting that "the agents either had or could have had, before they requested the warrant, all the Yahoo logs, which provided extensive information—whether a subscriber was offered e-mail delivery options; whether he elected a delivery option; whether he uploaded or posted any

---

images; when he subscribed; and whether he unsubscribed"). *Cf.* United States v. Froman, 355 F.3d 882, 884-91 (5th Cir. 2004) (upholding search warrant for member of group whose "singular goal . . . was to collect and distribute child pornography and sexually explicit images of children," when members could choose to automatically receive emails with attached images and Froman's interest in child pornography was shown by his chosen screen names, "Littlebuttsue" and "Littletitgirly").

[193] *Gourde*, 382 F.3d at 1006, 1011-13 (stating that screen name indicating sexual interest in children would add to probable cause determination).

[194] *See, e.g.*, United States v. Lacy, 119 F.3d 742, 745 (9th Cir. 1997) (probable cause found in child pornography case when affiant, based on her training and experience, explained that collectors and distributors of child pornography typically store it in their homes); United States v. Wagers, 339 F. Supp. 2d 934, 941 (E.D. Ky. 2004) ("In child pornography cases, courts have repeatedly recognized that collectors of child pornography tend to retain their materials."); United States v. Cox, 190 F. Supp. 2d 330, 333 (N.D.N.Y. 2002) (same); State v. Evers, 815 A.2d 432, 446, 448 (N.J. 2003) (probable cause to believe that pornographic images of children would be retained on computer due to retention habits of child pornographers); State v. Lindgren, 687 N.W.2d 60, 64-65 (Wis. App. 2004) (when defendant took nude photographs of a 14 year old female employee at work, touched her vaginal area, and had allegedly taken pictures of other female employees, and affiant detailed habits and characteristics of child molesters, including, *inter alia*, that they collect sexually explicit materials, rarely dispose of them, and record diaries of their encounters on, *inter alia,* their computers, probable cause existed to search home computer for photographic evidence of underage children of sexually explicit nature). *Cf.* United States v. Gourde, 382 F.3d 1003, 1006, 1011-13 (9th Cir. 2004) (merely because suspect was member of Internet child pornography site for at least two months insufficient to establish he had downloaded child pornography onto home computer, despite discussion of traits of child pornography collectors by affiant that included explanations that they "rarely if ever" dispose of pornography and that they use the Internet to share information and trade child pornography), *reh'g granted*, 416 F.3d 961 (9th Cir. 2005).

The reason why child pornography collectors retain their collections for long periods of time was explained by the court in *United States v. Lamb*, 945 F. Supp. 441, 460 (N.D.N.Y. 1996):

> Since the [child pornographic] materials are illegal to distribute and possess, initial collection is difficult. Having succeeded in obtaining images, collectors are unlikely to quickly destroy them. Because of their illegality and the imprimatur of severe social stigma such images carry, collectors will want to secret them in secure places, like a private residence. This proposition is not novel in either state or federal court: pedophiles, preferential child molesters, and child pornography collectors maintain their materials for significant periods of time.

*But see* United States v. Greathouse, 297 F. Supp. 2d 1264, 1272 (D. Or. 2003) allegations of staleness[195] and identifies the house as the place where the materials were viewed), and prior convictions involving sex offenses involving children or child pornography.[196]

---

(even though agent indicated in affidavit that child pornography collectors routinely maintain their materials for long periods of time, rejecting that assertion as sufficient because it appeared "to be based upon a generalized sense developed through informal conversations with other agents").

[195] *See, e.g.,* United States v. Hay, 231 F.3d 630, 636 (9th Cir. 2000) (probable cause that computer in suspect's home contained child pornography was not stale, even though information was six months old, due to affiant's explanation that collectors and distributors rarely if ever dispose of it and store it in secure place); United States v. Lacy, 119 F.3d 742, 745 (9th Cir. 1997) (probable cause not stale in child pornography case when based on information 10 months old because affiant, based on her training and experience, explained that collectors and distributors of child pornography "rarely if ever" dispose of such material); United States v. Wagers, 339 F. Supp. 2d 934, 941 (E.D. Ky. 2004) (collecting cases); Hause v. Commonwealth, 83 S.W.3d 1, 13-14 (Ky. App. 2002) (based on "hoarding" characteristics of child pornography collectors, information that was 178 days old not stale); United States v. Lamb, 945 F. Supp. 441, 460-61 (N.D.N.Y. 1996) (based, *inter alia*, on proposition that pedophiles, preferential child molesters, and child pornography collectors maintain their materials for significant period of time, five month delay from last transmission of child pornography to issuance of warrant did not render probable cause stale); State v. Schaefer, 668 N.W.2d 760, 767 (Wis. App. 2003) (information that suspect possessed child pornography in 1998, some of which went back to 1990, not stale based on protracted and continuous nature of habits of preferential child offenders, who rarely dispose of sexually explicit materials). *But cf.* United States v. Zimmerman, 277 F.3d 426, 433-34 (3d Cir. 2002) (probable cause based on viewing of pornographic video file on defendant's computer six months prior to execution of search warrant was stale, absent evidence that defendant had downloaded the video clip and absent evidence of continuous criminal activity); United States v. Greathouse, 297 F. Supp. 2d 1264, 1272-73 (D. Or. 2003) ("Carefully considering all of the factors present in this case, including the limited incriminating evidence, the absence of any evidence of intervening criminal activity, the absence of any evidence that [the suspect] was a pedophile, and the fact that computer equipment becomes obsolete very quickly, I find that the thirteen month delay in this case is simply too long. If a line must be drawn in internet child pornography cases, I find that the line is one year absent evidence of ongoing or continuous criminal activity.").

[196] *See, e.g.,* United States v. Wagers, 339 F. Supp. 2d 934, 941 (E.D. Ky. 2004); United States v. Fisk, 255 F. Supp. 2d 694, 706 (E.D. Mich. 2003) (when the defendant had prior conviction for unlawful sexual involvement with a minor, had wired money to purveyor of child pornography, and when the purveyor sold that pornography over the Internet, there was probable cause to believe that computer contained child pornography).

Another significant question is ascertaining the location of the computer that has distributed or received the child pornography. This difficulty arises because many individuals use computers in a variety of locations, including in an office and at home.[197] Persons accessing the Internet are assigned an Internet Protocol number, which does "*not directly* reflect the geographic street address of the office, residence, or building from which an individual accesses his email and/or the internet."[198] As a result, "law enforcement officials must conduct research and rely upon the addresses and data provided by internet providers, . . . as well as billing addresses for those service providers and/or credit card companies."[199]

Some courts will infer that the computer is located in the home from the Internet Protocol address assigned to the user's account. For example, in *United States v. Wagers*,[200] the court reasoned that, while the account holder

> had access to the internet from *many* locations . . . his residence and business locations are certainly the most likely and suspect locations through which he would have accessed the internet. The question, then, is not whether he did or did not access child pornography through the suspect sites from those physical addresses, but, rather, giving the Magistrate Judge's decision great deference, whether there is a "fair probability" that evidence or fruits of criminal wrongdoing would be

---

[197] *See, e.g.*, State v. Evers, 815 A.2d 432, 448 (N.J. 2003) ("Computers are in use in both homes and businesses, and, with the advent of the laptop, in almost every other conceivable place. Business people and students leave their homes with laptops, use them at other locations, and return home with them.").

[198] United States v. Wagers, 339 F. Supp. 2d 934, 940 (E.D. Ky. 2004). Internet protocol (IP) numbers are owned by Internet service providers; each number is unique to each computer while it is online. Terrence Berg, *Practical Issues in Searching and Seizing Computers*, 7 T.M. COOLEY J. PRAC. & CLINICAL L. 27, 37 n.22 (2004). However, IP numbers can be either "dynamic" or "static." A dynamic number, typically used by persons who have dial-up Internet service, changes each time the user goes online: "it is only good for that transaction, and then returns to the pool of numbers after the transaction is over." *Id.* On the other hand, a static IP number, which is more commonly used with cable and DSL connections, is permanently assigned to a customer. *Id.*

[199] *Wagers*, 339 F. Supp. 2d at 940.

[200] *Id.*

> found.[201]

As another example, in *State v. Brennan*,[202] although the suspect admittedly used his work laptop to view and store child pornography, the court found that there was a substantial basis for the magistrate's determination that probable cause existed to search the suspect's home computer based on the training and expertise of the affiant, who asserted that persons with an interest in child pornography tend to view it in their home. The court reasoned, in part, that "viewing and possessing child pornography is, by its nature, a solitary and secretive crime."[203] It accordingly believed that a "court could reasonably draw an inference that the suspect would keep the illicit images in a place considered safe and secret, like the home."[204] The court also relied on the transportable nature of laptops and stated that it was reasonable to infer "that the illicit images found on the laptop would also be found on [the suspect's] home computer."[205]

Screen names also help to identify who the person is. A "screen name" is an identity created by a user and may or may not have any correlation with the user's real name; an individual typically gains access to a screen name by supplying a password that is associated with that screen name.[206] Some courts will find probable cause to search the billing address associated with the screen name.[207] As one court has reasoned:

> The billing address of an account tied to a computer screen name may not be an absolute guarantee that the holder of the computer screen name used the computer at the billing ad-

---

[201] *Id.*

[202] 674 N.W.2d 200 (Minn. Ct. App. 2004).

[203] *Id.* at 206.

[204] *Id.*

[205] *Id.*

[206] United States v. Grant, 218 F.3d 72, 73 n.1 (1st Cir. 2000).

[207] *See, e.g.*, *Evers*, 815 A.2d at 446 ("[T]he billing address of the Internet screen name–a screen name that had e-mailed photographs of child pornography–was the logical place to search for evidence of the identity of the holder of the screen name and evidence of the crime.").

> dress to commit criminal activity, but there is a fair and logical inference that the computer will *probably* be found at that address and, if not, at least evidence of the identity of the holder of the screen name will be found there.[208]

Nonetheless, the court cautioned that it would prefer that law enforcement officials take additional steps to verify that the computer from which offending images were sent is located in the defendant's residence.[209]

Other courts have rejected the view that a registered screen name is sufficient to establish probable cause to search the subscriber's computer.[210] Instead, it has been suggested that additional information is needed, such as the fact that the suspect maintained a computer or computer-related equipment at the place to be searched that was capable of transmitting child pornography, the screen name required a particular password, the transmission of child pornography was to a unique Internet or ethernet address assigned to a particular computer at the location to be searched, or the person occupying the place to be searched had an "extreme" interest in young children or had access to Internet sites operated by entities that required those having access to maintain Internet-accessible child pornography.[211] Also relevant to the probable cause determination would be the habits of child pornography collectors, their propensity to collect child pornography and maintain the collection at home, and whether the suspect was a pedophile.[212]

---

[208] *Evers*, 815 A.2d at 446; *see also* United States v. Campos, 221 F.3d 1143, 1145 (10th Cir. 2000) (upholding validity of search warrant for defendant's residence after "[l]aw enforcement agents determined that AOL subscriber who used the name 'IAMZEUS' was [defendant]"); Hause v. Commonwealth, 83 S.W.3d 1, 4-5, 11-12 (Ky. Ct. App. 2001) (upholding validity of search warrant for residence that was supported by subscriber information obtained from Internet service provider through California search warrant and verification of address by Kentucky law enforcement officials).

[209] *Evers*, 815 A.2d at 446.

[210] *See, e.g.*, Taylor v. State, 54 S.W.3d 21 (Tex. App. 2001) (no probable cause to search computer for child pornography in Taylor's home when affidavit merely alleged that one image of child pornography sent over the Internet had been traced to screen name registered to Taylor).

[211] *See, e.g.*, Taylor v. State, 54 S.W.3d 21, 25-26 (Tex. App. 2001) (collecting cases); *see also* United States v. Bach, 400 F.3d 622, 627-28 (8th Cir. 2005) (probable cause existed to search defendant's home computer, even in absence of cross references of IP addresses provided by the ISP and his telephone records based, *inter alia*, on the fact that the user name employed to correspond to the

### *B. Consent*

#### 1. In General

Consent to search is a question of fact and is determined based on the totality of the circumstances.[213] The ultimate question turns on the voluntary nature of the consent.[214] The

---

minor was registered to defendant at his address), *cert. denied*, 2005 U.S. LEXIS 6585 (U.S., Oct. 3, 2005); United States v. Grant, 218 F.3d 72, 75 (1st Cir. 2000) (because use of password-protected account requires that user know password associated with account, fair probability that person using account is registrant).

[212] *See, e.g.,* Taylor v. State, 54 S.W.3d 21, 25-26 (Tex. App. 2001); *see also* Berg, *supra* note 198, at 42-45 (arguing that there are "good reasons" to follow the *Taylor* court's approach, including the fact that email headers can be forged, that the information given to an ISP regarding the user's billing address does not mean that a computer is present at that address, and that, with current technology, ISPs can determine the phone numbers and times when the account was accessed).

[213] Ohio v. Robinette, 519 U.S. 33, 40 (1996).

[214] *See, e.g.,* Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973) (viewing consent as an exception to warrant and probable cause requirements); United States v. White, 401 U.S. 745, 752 (1971); Alderman v. United States, 394 U.S. 165, 179 n.11 (1968); Hoffa v. United States, 385 U.S. 293, 302-03 (1966). Underlying consent principles is the Court's assumption of risk analysis. *See, e.g.,* United States v. Katz, 389 U.S. 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); United States v. Jacobsen, 466 U.S. 109, 118 (1984) (when individual reveals information to another, he assumes the risk that his confidant will reveal that information). Voluntariness–meaning the lack of coercion by the government agents—must be established. However, the consent need not be an informed one, which is to say that the person giving the consent need not know that he or she has the right to refuse, which is the essential holding of *Schneckloth*. The Amendment regulates the reasonableness of governmental actors, not the knowledge of private individuals. Hence, it is *reasonable* for a law enforcement officer to rely on the apparent consent of a person who seems authorized and competent to consent, regardless of whether or not the person is in fact authorized, competent, or otherwise making an informed choice. *See* Illinois v. Rodriguez, 497 U.S. 177, 183-89 (1990) (consent by person whom police reasonably believe to have common authority over premises validated search); United States v. Matlock, 415 U.S. 164, 171 (1974) (third party may consent to search if party has common authority or

principles regulating the permissibility of a search or seizure based on a claim of consent do not change in the context of computer searches.[215] However, computers present several challenges to the application of those principles.

### 2. Scope of Consent

A person may "delimit as he chooses the scope of the search to which he consents."[216] The government, in performing a search, cannot exceed the scope of the consent given. This is an objective inquiry: "what would the typical reasonable person have understood by the exchange between the officer and the suspect?"[217] Moreover, the scope of a consensual search is generally defined by its expressed object.[218] This is

---

other sufficient relationship to premises or effects).

[215] *See, e.g.,* United States v. Mabe, 330 F. Supp. 2d 1234, 1240 (D. Utah 2004) (rejecting assertion that defendant consented to search of computer after police falsely stated that they had search warrant); People v. Yuruckso, 746 N.Y.S.2d 33, 34-35 (N.Y. App. Div. 2002) (consent to search home computer valid, based on defendant's maturity, education, and other factors, even though police stated that, if he did not consent, they would obtain a search warrant and seize his work computer).

[216] Florida v. Jimeno, 500 U.S. 248, 252 (1991). *Cf.* United States v. Lemmons, 282 F.3d 920, 924-25 (7th Cir. 2002) (although suspect gave limited consent initially, his later consent to search computer made search valid); United States v. Greene, 56 M.J. 817, 822-23 (N-M. Ct. Crim. App. 2002) (when suspect signed form agreeing that agents could remove and retain his property or papers "which are desired for investigative purposes," agents did not exceed scope of consent when they seized his computer and discs and held them for three months).

[217] *Jimeno*, 500 U.S. at 251.

[218] *Id*; *see also* United States v. Raney, 342 F.3d 551, 558 (7th Cir. 2003) (seizure of "homemade" adult pornography within scope of consent to search for "'materials [that] are evidence in the nature of' child abuse, child erotica, or child exploitation" as it showed ability and intent to manufacture pornography depicting himself in sexual acts); United States v. Turner, 169 F.3d 84, 88-89 (1st Cir. 1999) (scope of defendant's permission to search apartment in connection with intruder's assault on neighbor exceeded when police accessed files on his computer because the police request would have been reasonably understood to be that they intended to search for physical evidence of the assault); State v. Brown, 813 N.E.2d 956, 960 (Ohio Ct. App. 2004) (scope of defendant's consent exceeded when police seized two computers from his home when he had merely given consent to look at computers); People v. O'Brien, 769 N.Y.S.2d 654, 656 (N.Y. App. Div. 2003) ("[T]he fact that the defendant's written consent was expressly limited to only the Comp USA computer and monitor located in his bedroom reveals

to say that consent "extends to the entire area in which the object of the search may be found and is not limited by the possibility that separate acts of entry or opening may be required to complete the search."[219] Thus, for example, troopers exceeded the scope of the driver's consent to search his vehicle for guns, drugs, money, or illegal contraband when they accessed the computer memory of a cellular phone to retrieve its electronic contents.[220] This is because a reasonable person would have understood the driver's consent to be limited to "search any containers inside the vehicle which might reasonably contain those specific items" and none of the objects sought would be found by accessing the phone's electronic contents.[221]

On the other hand, when a graduate student in computer science agreed to allow agents to search his entire home and to take his computer back to the FBI office for further examination, it was held that the student "would have realized that the examination of his computer would be more than superficial when the agents explained that they did not have the skills nor the time to perform the examination at his home."[222] Moreover, according to the court, "a graduate student in computer science would clearly understand the technological resources of the FBI and its ability to thoroughly examine his computer."[223] Given the lack of limitations put on the search by the student, his cooperation, and his expertise, the court believed it was reasonable for the agents to conclude that they had unlimited access to the computer.[224]

---

defendant's intent to maintain his privacy in all other contents of his bedroom," including another computer).

[219] United States v. Ross, 456 U.S. 798, 820-21 (1982); *see also Jimeno*, 500 U.S. at 251 (consent to search car included closed paper bag on floor of car); Commonwealth v. Hinds, 768 N.E.2d 1067, 1071 (Mass. 2002) (when defendant consented to search of his computer for electronic mail, valid search not limited to specific directories or locations on computer).

[220] Smith v. State, 713 N.E.2d 338, 343-44 (Ind. Ct. App. 1999).

[221] *Id.*

[222] United States v. Al-Marri, 230 F. Supp. 2d 535, 539-40 (S.D.N.Y. 2002).

[223] *Id.* at 540.

[224] *Id.*

### 3. Third Party Consent

The validity of third party consent depends on whether the person giving consent has either actual authority or apparent authority to consent.[225] In general, a third party may consent to a warrantless search when that party possesses "common authority over or other sufficient relationship to the premises or effects sought to be inspected."[226]

> Common authority is . . . not to be implied from the mere property interest a third party has in the property. The authority which justifies the third-party consent does not rest upon the law of property, with its attendant historical and legal refinements, but rests rather on mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched.[227]

The issue frequently arises in the context of shared computer use. The question, as with consent generally, turns on the person's access or control of the computer, regardless of whether the person is a spouse,[228] parent,[229] other family member,[230] house mate,[231] bailee,[232] systems administrator,[233] or other third party,[234] such as a computer repair person.[235]

---

[225] *See, e.g.,* United States v. Smith, 27 F. Supp. 2d 1111, 1115 (C.D. Ill. 1998).

[226] United States v. Matlock, 415 U.S. 164, 171 (1974); *see also* Frazier v. Cupp, 394 U.S. 731, 740 (1969) (rejecting inquiry into "metaphysical subtleties" of argument that, because joint user of duffle bag only had actual permission to use one compartment, he could not consent to search of whole bag).

[227] *Matlock*, 415 U.S. at 171 n.7.

[228] *See* Walsh v. State, 512 S.E.2d 408, 411-12 (Ga. Ct. App. 1999) (defendant's wife had authority to consent to search of computer that she purchased and was available for use by family).

[229] *See* People v. Blair, 748 N.E.2d 318, 324-25 (Ill. App. Ct. 2001) (father, who had no actual or apparent ownership of computer, could not validly consent to seizure of son's computer).

[230] *See* State v. Guthrie, 627 N.W.2d 401 (S.D. 2001) (son-in-law possessed common authority over computer and could validly consent to its seizure when he had unconditional access and control over it).

[231] *See* United States v. Smith, 27 F. Supp. 2d 1111, 1115-16 (C.D. Ill. 1998)

The presence of password-protected files is an important consideration in assessing a third party's authority to consent. For example, in *Trulock v. Freeh*,[236] the court held that a resident of a townhouse, Conrad, could not authorize the search of password-protected files of another resident, Trulock, on a computer that was jointly used when Conrad did not have access to the passwords. The court reasoned by analogy to the case of a mother who was found not to have authority to consent to the search of a locked footlocker in her son's room, which was located in a home they shared, and added: "By using a password, Trulock affirmatively intended to exclude Conrad

---

(housemate had authority to consent to search of defendant's computer, to which she had joint access and was located in common area of house; alternatively, government agents reasonably believed housemate could consent to search).

[232] *See* United States v. James, 353 F.3d 606, 614-15 (8th Cir. 2003) (bailee, who agreed to store disks and who had been later directed to destroy them, did not have actual or apparent authority to permit police to take and examine them).

[233] A "systems administrator" is the person "whose job is to keep [a computer] network running smoothly, monitor security, and repair the network when problems arise." CCIPS Manual, *supra* note 46, at 22. Those administrators "have 'root level' access to the systems they administer, which effectively grants them master keys to open any account and read any file on their systems." *Id.* As the CCIPS manual emphasizes, "the primary barrier to searching a network account pursuant to a system administrator's consent is statutory, not constitutional. Systems administrators typically serve as agents of 'provider[s] of electronic communication service' under the Electronic Communications Privacy Act ('ECPA'), 18 U.S.C. §§ 2701-2712." *Id.* Any attempt by law enforcement to obtain a system administrator's consent must comply with those provisions. *Id.* at 22-23. Regarding the Fourth Amendment, it is doubtful that a person using networks will be found to have a reasonable expectation of privacy in remotely stored files. *See* CCIPS Manual, *supra* note 46, at 23.

[234] *See* United States v. Meek, 366 F.3d 705, 711 (9th Cir. 2004) ("Like private phone conversations, either party to a chat room exchange has the power to surrender each other's privacy interest to a third party.").

[235] United States v. Barth, 26 F. Supp. 2d 929, 938 (W.D. Tex. 1998) (computer repair person does not have actual authority to consent to search of customer's hard drive, having "possession of the unit for the limited purpose of repair" and did not have apparent authority when police knew his status).

[236] 275 F.3d 391 (4th Cir. 2001).

and others from his personal files."[237] On the other hand, the lack of passwords to protect files has been held to defeat a claim that the defendant had exclusive control of a computer and that his housemate did not have authority to consent to search.[238]

### *C. Particularity Claims*

#### 1. In General

The Fourth Amendment requires that a search warrant describe with particularity "the place to be searched, and the persons or things to be seized."[239] The particularity requirement prevents a "general, exploratory rummaging in a person's belongings"[240] and the seizure of one thing under a warrant describing another.[241] It also "'assures the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search.'"[242] Although the Supreme Court has observed that, "[a]s to what is to be taken, nothing is left to the discretion of the officer executing the warrant,"[243] this admonition has not been applied strictly by courts.[244] A warrant satisfies the particularity requirement if it enables the executing officer to identify with reasonable certainty those items that the issuing magistrate has authorized him to seize.[245] This is determined, *inter alia*,[246] by the nature of the activity charged[247] and the nature of the objects to be seized.[248] Without a sufficiently specific warrant, the search is considered warrantless.[249]

---

[237] *Id.* at 403.

[238] United States v. Smith, 27 F. Supp. 2d 1111, 1116 (C.D. Ill. 1998).

[239] U.S. CONST. amend. IV.

[240] Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

[241] Marron v. United States, 275 U.S. 192, 196 (1927); *see also* LAFAVE, *supra* note 95, § 4.6(a) at 605 (underlying purposes of the particularity requirement are to prevent general searches and to prevent the "seizure of objects under the mistaken assumption that they fall within the magistrate's authorization").

[242] Groh v. Ramirez, 540 U.S. 551, 561 (2004) (quoting United States v. Chadwick, 433 U.S. 1, 9 (1977)).

[243] *Marron*, 275 U.S. at 196.

[244] *See, e.g.,* Davis v. Gracey, 111 F.3d 1472, 1478 (10th Cir. 1997) (a "warrant that describes the items to be seized in broad or generic terms may be valid when the description is as specific as the circumstances and the nature of the activity under investigation permit"); United States v. Riley, 906 F.2d 841, 845 (2d Cir. 1990) ("Once a category of seizable papers has been adequately described, with the description delineated in part by an illustrative list of seizable items, the Fourth Amendment is not violated because the officers executing the warrant must exercise some minimal judgment . . . .").

### 2. Varieties of Computer Searches

There are two varieties of computer searches: one is to seize the equipment, that is, the computer hardware and software; the other is to obtain the data contained in the computer equipment, including on hard drives and various storage devices, such as floppy disks. Helpful analysis in recognizing this distinction is contained in *In re Grand Jury Subpoena Duces Tecum Dated November 15, 1993*.[250] Although decided under Federal Rule of Procedure 17(c) rather than under the Fourth Amendment, the court was presented with a subpoena that demanded that X Corporation provide the grand jury with the central processing unit, including the hard drive, of any computers supplied by the corporation to specified employees. The subpoena also demanded all computer-accessible data, including floppy diskettes created by those employees or their assistants. The court noted that, not only were corporate records within the scope of the subpoena, so were personal documents. The grand jury was investigating securities trading activities and obstruction of justice. The court observed:

---

[245] Maryland v. Garrison, 480 U.S. 79, 84 (1987).

[246] *See* LAFAVE *supra* note 95, § 4.6(a) at 609-13 (summarizing many of the general principles that can be distilled from the decided cases).

[247] *See, e.g.*, Andresen v. Maryland, 427 U.S. 463, 479-80 (1976) (phrase seeking all evidence was not general when modified by sentence referring to specific crime); United States v. Johnson, 541 F.2d 1311, 1314 (8th Cir. 1976); United States v. Abbell, 963 F. Supp. 1178, 1196 (S.D. Fla. 1997).

[248] LAFAVE, *supra* note 95, § 4.6(a) at 609-11; *see also* State v. Wible, 51 P.2d 830, 836 (Wash. App. 2002) ("Courts evaluating alleged particularity violations distinguish between inherently innocuous items, such as [a] computer, and inherently illegal property, such as controlled dangerous substances. . . . Innocuous items require greater particularity.").

[249] *Groh*, 546 U.S. at 558.

[250] 846 F. Supp. 11 (S.D.N.Y. 1994).

> The subpoena at issue here is not framed in terms of specified categories of information. Rather, it demands specified information storage devices–namely, particular computer hard drives and floppy disks that contain some data concededly irrelevant to the grand jury inquiry. . . . If the categories of materials properly are seen to be hard disk drives and floppy disks, then . . . it is highly probable that these devices will contain some relevant information. If, on the other hand, the categories of materials properly are seen to be the various types of documents contained on these devices, then the subpoena would be unreasonably broad because there are easily separable categories of requested documents that undoubtedly contain no relevant information.[251]

Concluding that the grand jury was actually seeking documents and not the devices that stored them, the court held that the subpoena was too broad.[252] Similarly, under the Fourth Amendment, it must be determined whether the computer is a mere storage device for data[253] or whether the equipment[254] is the object sought.

### *a. Searches for Computer Equipment*

In the context of warrants issued to seize computer software and hardware,[255] the courts have often found fairly generic descriptions of the items to be seized to be sufficient.[256] For example, merely labelling the objects to be seized as evidence of, or an instrumentality[257] of, a crime as "computer equipment"[258] or even "equipment"[259] relating to a specific crime has sufficed. Of course, if computer equipment has been stolen and that specific equipment is the object of the search, it would have to be described with sufficient particularity to identify it.[260]

---

[251] *Id.* at 12.

[252] *Id.* at 13-14.

[253] *See, e.g.,* United States v. Gawrysiak, 972 F. Supp. 853, 860-61 (D.N.J. 1997) (approving warrant to search for documents related to wire fraud investigation, including records stored in magnetic or electronic forms), *aff'd,* 178 F.3d 1281 (3d Cir. 1999).

[254] *See, e.g.,* Arkansas Chronicle v. Easley, 321 F. Supp. 2d 776, 793 (E.D. Va. 2004) (comparing seizure of computer equipment in child pornography cases, where those devices are considered instrumentalities of crime, with computers that are tools of journalist's trade that may or may not contain evidence); United States v. Hunter, 13 F. Supp. 2d 574, 584-85 (D. Vt. 1998) (warrant authorizing wholesale seizure of computers and related devices, without specifying crime for which computers were sought, violated particularity requirement).

[255] *See, e.g.,* CCIPS Manual, *supra* note 46, at 63-64 (discussing that, under Fed. R. Crim. P. 41(b), agents may obtain search warrants to seize computer hardware if the hardware is contraband, evidence, or an instrumentality or fruit of a crime).

### *b. Searches for Data*

As discussed at the beginning of this article,[261] there are two principal approaches to searches involving electronic data stored on computers, that is, whether a computer is a form of a container and the data in electronic storage mere forms of documents or whether such searches for data require a "special approach." Perhaps the most significant consequence of those competing views is in the application of the Fourth Amendment's particularity requirement. If data is considered a form of a document and the computer is just a container holding that document, the traditional limitations on document searches apply.[262] On the other hand, if the court rejects such an analogy and adopts the "special approach" to searches of data on computers, then unique limitations are likely to be imposed.[263]

---

[256] *See, e.g.,* State v. Lehman, 736 A.2d 256, 260-61 (Me. 1999) (collecting cases).

[257] *See, e.g.,* Arkansas Chronicle v. Easley, 321 F. Supp. 2d 776, 793 (E.D. Va. 2004) (comparing seizure of computer equipment in child pornography cases, where those devices are considered instrumentalities of crime, with computers that are tools of a journalist's trade).

[258] *See* United States v. Lacy, 119 F.3d 742, 745-47 (9th Cir. 1997), *cert. denied,* 523 U.S. 1101 (1998) (upholding warrant issued for search of "computer equipment and records" that resulted in seizure of computer, more than 100 computer disks, and documents when government knew that suspect had downloaded child pornography but did not know where the images had been stored, with the court concluding that "this type of generic classification is acceptable 'when a more precise description is not possible'"); United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999), *cert. denied,* 527 U.S. 1011 (1999) (observing that warrant issued for "[a]ny and all computer software and hardware, . . . computer disks, disk drives" is easily administered by seizing officer based on objective criteria whether item is computer equipment).

[259] Davis v. Gracey, 111 F.3d 1472, 1478-79 (10th Cir. 1997) (computers, monitors, keyboards, modems, CD-ROM drives, and changers were within the meaning of warrant that directed officers to search for "equipment . . . pertaining to the distribution or display of pornographic material").

[260] *See, e.g.,* State v. Tanner, 534 So. 2d 535, 537 (La. App. 1988) (when defendant illegally copied software and other materials belonging to First Page Beeper Services, warrant not overbroad that authorized seizure of "all other computer related software" that bore the name "First Page Beepers"). *But cf.* State v. Wade, 544 So. 2d 1028, 1029-30 (Fla. App. 1989) (warrant, which resulted in seizure of 53 items, that authorized seizure of "computer equipment and business records" that had been stolen from Controlled Data Corporation was sufficiently particular when it incorporated by reference exhibit listing three specific items but was not limited to those items).

[261] *See* discussion *supra* at 197-205.

### *D. Plain View*

The permissible scope of a search is usually determined by the objects sought under the warrant. If small objects (such as fibers or bullets) are the target of the search, law enforcement officials can look anywhere such an object may be hidden; if only large objects are sought, the officials can only look where that size of object can be concealed. In executing a search, it is not uncommon for the police to encounter objects that are incriminating or have evidentiary value for which they did not have prior authority to search or seize. Under such circumstances, the plain view doctrine may justify seizure of the object. That doctrine has three requirements: a prior valid intrusion; observing an object in plain view; and the incriminating character of the object must be immediately apparent.[264]

In the context of searches of computers for electronic evidence, if the police are otherwise validly in position to observe a computer screen, their observations of what is depicted on the screen will be considered in plain view.[265] As to observations of the contents of unopened files, what is in plain view is determined by whether the court accepts the view that data are mere types of document searches,[266] and hence the official can look at all data to ascertain its value when executing a warrant to search for documents,[267] or whether the court takes a spe-

---

[262] *See* discussion *supra* at 197-201.

[263] *See* discussion *supra* at 202-20.

[264] Horton v. California, 496 U.S. 128, 136-37 (1990). There is no requirement that the spotting of the object be inadvertent. *Id.*; *see also* Ivatury v. State, 792 S.W.2d 845, 851 (Tex. Ct. App. 1990) (based on warrant to search safety deposit box during espionage investigation, discovery of special type of computer tape in box used in defense industry in plain view).

[265] *See* State v. Mays, 829 N.E.2d 773, 779 (Ohio Ct. App. 2005) (observations

---

of information on computer screen during consent search of home in plain view); United States v. Tanksley, 50 M.J. 609, 620 (N-M. Ct. Crim. App. 1999) (observations of information on computer screen made during search of office were in plain view); People v. Blair, 748 N.E.2d 318, 323 (Ill. App. 2001) (when police observed 'bookmarks with references to teenagers and so forth,' they did not have probable cause to believe that computer contained child pornography); State v. One Pioneer CD-ROM Changer, 891 P.2d 600, 604-05 (Okla. Civ. App. 1995) (during execution of search warrant based on allegations that suspect was distributing pornographic material, police observations of computer monitor "displaying the words 'viewing' and/or 'copying' with descriptions such as 'lesbian sex' and/or 'oral sex'" established that the equipment and its possible criminal use were in plain view). *Cf.* United States v. Turner, 169 F.3d 84, 88 (1st Cir. 1999) (observation of officer during consensual search of apartment of photograph of a nude woman on computer screen did not justify search of computer for other incriminating files); State v. Brown, 813 N.E.2d 956, 960-62 (Ohio Ct. App. 2004) (incriminating nature of computers and their contents not immediately apparent based on mere observation of two computers in defendant's house, with no pornography displayed on screen, when police merely knew that pornographic material had been printed from some computer). Of course, if there is no prior intrusion at all, that is, no prior search or seizure within the meaning of the Fourth Amendment, then an officer's use of her sight to observe something is not a search. *See, e.g.,* United States v. David, 756 F. Supp. 1385, 1390 (D. Nev. 1991) (agent's looking over defendant's shoulder to see password for defendant's computer not search).

[266] *See* discussion *supra* at 198-206.

[267] *See, e.g.,* United States v. Gray, 78 F. Supp. 2d 524, 531 n.11 (E.D. Va. 1999) (when agent is engaged in "systematic search" of computer files pursuant to warrant, any evidence discovered could be seized under plain view doctrine); Commonwealth v. Hinds, 768 N.E.2d 1067, 1072 (Mass. 2002) (police had right to open file that officer believed contained child pornography based on file's name during search of computer for email; accordingly, child pornography was in plain view); State v. Schroeder, 613 N.W.2d 911, 916 (Wis. Ct. App. 2000) (rejecting limitations on search based on file names and concluding that, during systematic search of all user-created files in executing search warrant for evidence of online harassment and disorderly conduct, opening file containing child pornography in plain view); Frasier v. State, 794 N.E.2d 449, 462-66 (Ind. Ct. App. 2003) (rejecting limitations on a search based on file names and extensions, and concluding that plain view doctrine applied when police opened file and observed child pornography during execution of warrant permitting police to examine notes and records for evidence of drug trafficking). *Cf.* United States v. Wong, 334 F.3d 831, 838 (9th Cir. 2003) (under warrant permitting search of graphic files for evidence of murder, observations of files containing child pornography in plain view); Unit-

cial approach[268] to computer searches and imposes limitations on the search by, for example, file name or file type.[269] It also depends on how the court defines the relevant container.[270]

### *E. Execution Issues*

#### 1. On-site/Off-site Searches; Intermingled Documents

One question that has often arisen is whether the government may remove the computer, including its hard drive and disks, to the police station for detailed forensic examination. Answering this question, courts have fairly consistently held that, due to the intermingling of legitimate and illegitimate items, the technical difficulty of examination, and the volume of information seized, temporary seizures of the computer and removal off site for examination are permitted.[271] Underlying

---

ed States v. Tucker, 305 F.3d 1193, 1202-03 (10th Cir. 2002) (parole agreement authorized search of computer; upon viewing child pornography on it, plain view permitted seizure).

[268] *See* discussion *supra* at 202-20.

[269] *See* United States v. Carey, 172 F.3d 1268, 1272-75 (10th Cir. 1999) (opening of files containing child pornography, at least after first file was opened, during execution of search warrant for documentary evidence relating to drug dealing, not justified by plain view doctrine because files were "closed" and "unambiguously" named). *Cf.* United States v. Abbell, 914 F. Supp. 519, 520-21 (S.D. Fla. 1995) (in criminal prosecution where large volume of computer generated data seized from defendant's law office, special master would determine whether documents and data were responsive to warrant or fell within exception to warrant requirement); United States v. Maxwell, 45 M.J. 406, 422 (C.A.A.F. 1996) (where officer used personal computer to transport obscenity and child pornography, plain view doctrine inapplicable to search of computer files under screen name not listed in warrant); *see also* Brenner & Frederiksend, *supra* note 18, at 89-106 (advocating significant restrictions on application of plain view doctrine to computer searches).

[270] *See* discussion *supra* at 233-44.

[271] *See, e.g.*, United States v. Walser, 275 F.3d 981, 985 (10th Cir. 2001) (observing that seizure is appropriate in variety of circumstances, including "the impracticality of on-site sorting" and because "computer evidence is vulnerable to tampering or destruction"); Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001) (due to "technical difficulties of conducting a computer search in a suspect's home," permissible to seize computers and their contents and remove to allow police to locate relevant data); United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000) (upholding, in child pornography case, warrant authorizing seizure of computer system because of the "time, expertise, and controlled environment required for a

the courts' analysis is the fundamental premise that "current

---

proper analysis"); *Upham*, 168 F.3d at 535 ("As a practical matter, the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the images. A sufficient chance of finding some needles in the computer haystack was established by the probable-cause showing in the warrant application; and a search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for a weapon or drugs."); United States v. Sissler, 966 F.2d 1455 (6th Cir. 1992), *cert. denied*, 506 U.S. 1079 (1993) (police permitted to remove computers from defendant's residence to continue search off-site); Mahlberg v. Mentzer, 968 F.2d 772, 775 (8th Cir. 1992) (seizure of 160 computer disks permissible when searching for two computer files because of possibility that computer was 'bobby-trapped' to erase itself and because it was unknown which disks contained the files); United States v. Schandl, 947 F.2d 462, 465-66 (11th Cir. 1991), *cert. denied,* 504 U.S. 975 (1992) (in tax evasion case, which requires "careful analysis and synthesis of a large number of documents," it might be more disruptive to conduct thorough search of each individual document and computer disk before removing it; to insist on such a practice would substantially increase time to conduct search, thereby aggravating its intrusiveness); United States v. Maali, 346 F. Supp. 2d 1226, 1246 (M.D. Fla. 2004) (("Warrants authorizing seizure of computer equipment for later off-site search of their contents for evidence . . . have been upheld, especially where, as here, the supporting affidavit explained the reason such off-site analysis was necessary."); United States v. Leveto, 343 F. Supp. 2d 434, 449-50 (W.D. Pa. 2004) (in large tax fraud scheme, involving many documents and computer files, off-site inspection permissible); United States v. Albert, 195 F. Supp. 2d 267, 278-79 (D. Mass. 2002) (upholding off-site search because "the mechanics of searching a hard drive by viewing all of the information it contains cannot be readily accomplished on site"); United States v. Hunter, 13 F. Supp. 2d 574, 583 (D. Vt. 1998) ("Often it is simply impractical to search a computer at the search site because of the time and expertise required to unlock all sources of information."); United States v. Yung, 786 F. Supp. 1561, 1569 (D. Kan. 1992) (computer files "clearly could not be individually reviewed prior to completion of the search"); People v. Gall, 30 P.3d 145, 154-55 (Colo. 2001) (seizure of computers and later search off site upheld). *Cf.* United States v. Gawrysiak, 972 F. Supp. 853, 866 (D.N.J. 1997) ("A reasonable-search of computer files may include copying those files on to a disk on the scene, for later time-consuming review of the index of documents to cull the relevant time periods and subject matters while returning the remainder."), *aff'd,* 178 F.3d 1281 (3d Cir. 1999); CCIPS Manual, *supra* note 46, at 64-66 (discussing possible search strategies where the hardware is a mere storage device for electronic evidence). *But see* Brenner & Frederiksen, *supra* note 18, at 45-89 (extensively analyzing the off/on site issue and advocating the view that an off-site search "should be treated as an "unusual measure" and specifically authorized by a magistrate, *id.* at 76, and that computer hardware cannot be seized absent explanation in warrant application of technical reasons why the search cannot be conducted on-site or conducted off-site using forensic back-up copies of data, *id.* at 75).

technology does not permit proper on-site examination of computer files."[272] For example, in *United States v. Hill*,[273] the court concluded that the police were not required to bring with them equipment capable of reading computer storage media and an officer competent to operate it; the court observed:

> Doing so would have posed significant technical problems and made the search more intrusive. . . . Because computers in common use run a variety of operating systems—various versions or flavors of Windows, Mac OS and Linux, to name only the most common—police would have had to bring with them a computer (or computers) equipped to read not only all of the major media types, but also files encoded by all major operating systems. Because operating systems, media types, file systems and file types are continually evolving, police departments would frequently have to modify their computers to keep them up-to-date. This would not be an insuperable obstacle for larger police departments and federal law enforcement agencies, but it would pose a significant burden on

---

[272] United States v. Al-Marri, 230 F. Supp. 535, 541 n.3 (S.D.N.Y. 2002); *see also* United States v. Campos, 221 F.3d 1143, 1147 (10th Cir. 2000) (quoting FBI agent's explanation as to why it was not usually feasible to search for particular computer files in person's home, which included the volume of information, user attempts to conceal criminal evidence, need for an expert examiner, controlled environment, wide variety of computer hardware and software, and vulnerably of evidence to tampering or destruction); United States v. Greene, 56 M.J. 817, 823-24 (N-M. Ct. Crim. App. 2002) (discussing expert witness testimony on effective forensic analysis, including danger of destruction of evidence when conducting on-site examinations and need for off-site analysis to protect evidence); *Gall*, 30 P.3d at 154-55 ("In addition to the problems of volume and commingling, the sorting of technological documents may require a search to be performed at another location 'because that action requires a degree of expertise beyond that of the executing officers,' not only to find the documents but to avoid destruction or oversearching."). *Cf.* United States v. Greathouse, 297 F. Supp. 2d 1264, 1269, 1275 (D. Or. 1275) (although acknowledging that numerous cases have upheld the "wholesale seizure of computers and computer disks and records for later review for particular evidence as the only reasonable means of conducting a search," observing "that this may not always be true due to technological developments" and stating that, in the appropriate situation, "there may well be an obligation" to use a computer forensics program "to more narrowly tailor the search and seizure"); *Hunter*, 13 F. Supp. 2d at 583 ("until technology and law enforcement expertise render on-site computer records searching both possible and practical, wholesale seizures, if adequately safeguarded, must occur").

[273] 322 F. Supp. 2d 1081 (C.D. Cal. 2004).

> smaller agencies.
>
> Even if the police were to bring with them a properly equipped computer, and someone competent to operate it, using it would pose two significant problems. First, there is a serious risk that the police might damage the storage medium or compromise the integrity of the evidence by attempting to access the data at the scene. As everyone who has accidentally erased a computer file knows, it is fairly easy to make mistakes when operating computer equipment, especially equipment one is not intimately familiar with. The risk that the officer trying to read the suspect's storage medium on the police laptop will make a wrong move and erase what is on the disk is not trivial. Even if the officer executes his task flawlessly, there might be a power failure or equipment malfunction that could affect the contents of the medium being searched. For that reason, experts will make a back-up copy of the medium before they start manipulating its contents. Various other technical problems might arise; without the necessary tools and expertise to deal with them, any effort to read computer files at the scene is fraught with difficulty and risk.
>
> Second, the process of searching the files at the scene can take a long time. To be certain that the medium in question does *not* contain any seizable material, the officers would have to examine every one of what may be thousands of files on a disk—a process that could take many hours and perhaps days. Taking that much time to conduct the search would not only impose a significant and unjustified burden on police resources, it would also make the search more intrusive. Police would have to be present on the suspect's premises while the search was in progress, and this would necessarily interfere with the suspect's access to his home or business. If the search took hours or days, the intrusion would continue for that entire period, compromising the Fourth Amendment value of making police searches as brief and non-intrusive as possible.[274]

Because of these considerations, the court concluded that the police were not required to examine the electronic storage media at the scene to determine which contained child pornography and which did not but were, instead "entitled to seize all such media and take them to the police station for examination by an expert."[275]

---

[274] *Id.* at 1088-89.

Nonetheless, courts have expressed concerns about such wholesale seizures due to the disruption of businesses, professional practices, and personal lives that such seizures entail.[276] Accordingly, courts have been cautious in their approval of such practices.[277] Some urge that the government copy the data and return the equipment as soon as possible.[278] A few courts appear to require a second warrant before searching when the government seizes intermingled documents.[279]

---

[275] *Id.* at 1089.

[276] *Hunter*, 13 F. Supp. 2d at 583.

[277] *See, e.g.*, *Upham*, 168 F.3d at 535.

[278] *Hunter*, 13 F. Supp. 2d at 583. *Cf. Leveto*, 343 F. Supp. 2d at 441 (in large tax fraud scheme, involving many documents and computer files, factually describing how executing officials took "considerable steps" to minimize "upheaval" of veterinarian's business, including copying computer files rather than removing computers). *But cf.* Malapanis v. Regan, 335 F. Supp. 2d 285, 291 (D. Conn. 2004) (failure of police to return computer equipment does not implicate Fourth Amendment; it is, instead, analyzed under procedural due process); LM Bus. Assoc. v. Ross, No. 04-CV-612CJS 2004 WL 2609182, at *5 (W.D.N.Y. Nov. 17, 2004) (same).

[279] *See, e.g.*, United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999). This requirement is based on precedent requiring a second warrant when the police seize intermingled documents. *See* United States v. Shilling, 826 F.2d 1365, 1369-70 (4th Cir. 1987) (although stating that "we cannot easily condone the wholesale removal of file cabinets and documents not covered by the warrant," concluding that there were legitimate practical concerns that prompted the removal of file cabinets and observing that seizure not based on intent to engage in fishing expedition); United States v. Tamura, 694 F.2d 591, 595-96 (9th Cir. 1982) (suggesting that when documents are so intermingled that sorting on site is not feasible, Fourth Amendment violations can be avoided by sealing documents and obtaining additional search warrant). Other courts reject that requirement for document searches. *See, e.g.*, United States v. Hargus, 128 F.3d 1358, 1363 (10th Cir. 1997) (seizure of entire file cabinet permissible, including intermixed warrant-specified and unspecified documents). Some courts have raised these concerns in the computer context but have not specifically addressed the issue. *See, e.g.*, *Upham*, 168 F.3d at 536 ("This problem arises in a variety of different contexts and in many permutations; matters of degree are involved and there is probably no single rule that resolves all such situations."). *Cf. Hill*, 321 F. Supp. 2d at

### 2. Use of Experts

Because of the complicated nature of the evidence and equipment that computer-related searches give rise to, governmental authorities sometimes use computer experts to facilitate the execution of a search warrant. Challenges to the use of such experts, although few, have been consistently rejected.[280] The civilian, of course, must be "serving a legitimate investigative function,"[281] including using his or her special expertise to identify "property of a technical nature not generally familiar to law enforcement officers."[282] Approval has even extended to situations where the private experts performed the search outside of the presence of law enforcement officials.[283]

### 3. Deleted Files

When a computer user "deletes" a file, the data that was contained in that file may remain in the computer memory:

> Most word processing programs use some form of a recycle bin, into which documents are transferred when deleted.

---

1090 ("The warrant here authorized precisely such a seizure of intermingled materials that are difficult and time-consuming to separate on-site. That the officer seeking the warrant did not make a specific showing to this effect is of no consequence: The difficulties of examining and separating electronic media at the scene are well known. It is doubtless with these considerations in mind that the state court judge authorized seizure of all of defendant's storage media, not merely those containing contraband or evidence of crime."); *Gall*, 30 P.3d at 154-55 (observing that the problem of "properly limiting a search of the contents of a lawfully seized computer" was not at issue because search pursuant to second, more detailed warrant).

[280] *See, e.g.,* Belleville v. Town of Northboro, 375 F.3d 25, 32 (1st Cir. 2004) ("Federal constitutional law does not proscribe the use of civilians in searches."); *Hill*, 322 F. Supp. 2d at 1088 n.10 (recognizing that experts may be advisable to limit search); United States v. Schwimmer, 692 F. Supp. 119, 126-27 (E.D.N.Y. 1988) (summarily rejecting challenge to use of computer expert).

[281] *Belleville*, 375 F.3d at 32.

[282] *Wade*, 544 So. 2d at 1030-31 (computer experts from company from which computer equipment was stolen assisted in identifying equipment); *accord Belleville*, 375 F.3d at 32.

[283] *See* United States v. Bach, 310 F.3d 1063, 1066-68 (8th Cir. 2002) (private Internet service provider employees searched suspect's email), *cert. denied*, 538 U.S. 993 (2003).

> Thus, a computer is also like a wastebasket of discarded material. In order to attempt to permanently delete such documents, the recycle bin must be emptied. However, even emptying the recycle bin may not actually delete the document or file because the information may still remain on the computer's hard drive.
>
> The intentional deletion of a file does not permanently erase the file. Instead, the computer internally marks the file as not needed, and clears space for storage of other files. The erasure of information only occurs when the computer overwrites the file with another file. Even then, fragments of information may be retrievable if the entire file is not overwritten. Furthermore, word processing programs may have saved portions or versions of documents regardless of whether the user intentionally saves the final version.
>
> Thus, in general, a file or document may not be removed from the hard drive of a computer until it is reformatted. However, even then, it may be possible to partially recover documents or files removed from a hard drive, depending on how the drive was reformatted. Further, the potential for deleted material to be stored on a hard drive, with or without intentional saving by the user, is not limited to word processing documents, but applies to other programs and functions of a computer as well.[284]

Because technicians can often recover much of that data using electronic search technology, courts have confronted a variety of issues regarding the admissibility of such "deleted" data. Some courts have addressed–and rejected–the government claim that the files have been abandoned.[285] The analogy of deletion of a file to putting one's trash out in the street is flawed, according to one court, because in the latter situation, but not the former, every passerby can search the trash.[286]

---

[284] *Gall*, 30 P.3d at 161 (Martinez, J., dissenting) (citations omitted). *See, e.g., Upham*, 168 F.3d at 537 (rejecting scope argument and asserting that recovery of deleted files no different than "pasting together scraps of a torn-up ransom note").

[285] *See, e.g., Upham*, 168 F.3d at 537 n.3. *Cf.* United States v. Angevine, 281 F.3d 1130, 1135 (10th Cir. 2002) (when defendant did not have access to data he previously attempted to delete on university owned computer, he had no reasonable expectation of privacy in that data).

On the other hand, defendants have claimed that the recovery of deleted files is outside the scope of a warrant;[287] the assertion is that a second warrant is required or the scope of the original warrant has been exceeded because the "deletion" of the documents creates a new and legally different expectation of privacy protected by the Amendment.[288] Rejecting such a claim, one court has reasoned that an "attempt to secrete evidence of a crime is not synonymous with a legally cognizable expectation of privacy."[289] The court analogized the situation to a paper tablet and a diary recorded in a private code, both of which may be subjected to scientific analysis after seizure pursuant to a warrant; the court concluded that no second warrant was required "before subjecting legally seized physical evidence to scientific testing and analysis to make it divulge its secrets."[290]

## V. CONCLUSION

Courts are increasingly confronting the problems associated with adapting Fourth Amendment principles to modern technology.[291] Supreme Court jurisprudence, developed to regulate traditional search and seizure practices, presents conceptual problems when applied to the world of cyber-space and electronically stored evidence. Some authorities are reluctant to accept–or outright reject–analogies to physical world searches and seizures. This article concludes, however, that there is nothing "special" in the nature of computer searches that differentiate them in any principled way from other document and container searches. Assuming the validity of the document/container analogy, however, also requires recognition of what the relevant container is, which has significance for application of the plain view and private search doctrines. Traditional Fourth Amendment principles can be translated to the search of electronic evidence. Although one may dispute the correctness of some of the Supreme Court's development of Fourth Amendment principles, as I have elsewhere, there is nothing *sui generis* where the target of the search or seizure is a computer or other device that contains electronic evidence.

---

[286] *Upham*, 168 F.3d at 537 n.3.

[287] *See, e.g., id.* at 537 (recovery of deleted files no different than "pasting together scraps of a torn-up ransom note").

[288] Commonwealth v. Copenhefer, 587 A.2d 1353, 1356 (Pa. 1991).

[289] *Id.*

[290] *Id.*

[291] *See generally Symposium: The Effect of Technology on Fourth Amendment Analysis and Individual Rights*, 72 MISS. L.J. 1 (2002).

# COMPUTER SEARCHES OF PROBATIONERS—Diminished Privacies, "Special Needs" & "'*Whilst*' *Quiet* Pedophiles"—Plugging the Fourth Amendment into the "Virtual Home Visit"

*Marc M. Harrold*[*]

## INTRODUCTION

The Fourth Amendment, expressly designed to afford privacy[1] to an individuals' "persons, houses, papers, and effects"[2] must now delineate the limits of constitutionally-protected privacies against unreasonable searches and seizures in a world that is spacial instead of geographic; digital instead of physical. The evolution from an industrial age to an information age is no less dramatic than from an agrarian society to an industrial one more than a century ago.[3] These "switches

---

[*] Counsel for National Programs and Visiting Professor of Law, National Center for Justice and the Rule of Law, University of Mississippi School of Law. J.D., University of Mississippi School of Law; B.A., Clemson University. This article was supported by the National Center for Justice and the Rule of Law (NCJRL). The NCJRL at the University of Mississippi School of Law is supported by Grant No. 2000-DD-VX-0032, awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention and the Office of Victims of Crime. Points of view or opinions in this article are those of the author and do not represent the official position of the United States Department of Justice or the National Center for Justice and the Rule of Law. I extend my appreciation to Thomas K. Clancy, Orin Kerr, Donald R. Mason, Jack Nowlin and Scott Sundby for their willingness to review a draft of this article and for their comments, suggestions, and insight.

[1] I use the term "privacy" to describe the protections of the Fourth Amendment because of the United States Supreme Court's general and current reliance on "privacy" as its primary basis for analysis. *See* United States v. Knights, 534 U.S. 112, 118-19 (2001) ("The touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined 'by assessing, on the one hand, the degree to which it intrudes upon an individual's *privacy* . . . .'") (emphasis added) (citations omitted); *see also* Melissa Arbus, Note, *A Legal U-Turn: The Rehnquist Court Changes Direction and Steers Back to the Privacy Norms of the Warren Era*, 89 VA. L. REV. 1729 (2003) (discussing how cases involving modern surveillance (namely *Bond* and *Kyllo*) indicate the Rehnquist's Court's return back to a more "privacy"-focused Fourth Amendment doctrine.). I agree with

---

Thomas K. Clancy that, especially with regards to emerging technology, *security* is the best measure of what is actually protected by the Fourth Amendment. *See* Thomas K. Clancy, Essay, *Coping with Technological Change:* Kyllo *and the Proper Analytical Structure to Measure the Scope of Fourth Amendment Rights,* 72 MISS. L.J. 525, 536 (2002) ("The Fourth Amendment speaks of the right to be secure and, in my view, is the proper measure of the protection afforded by the Amendment.").

[2] U.S. CONST. amend. IV. The Fourth Amendment:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

*Id.*

[3] From the Court's earliest consideration of new technology, certain Justices have been cognizant of the expansive governmental surveillance power which could result and the challenge it would pose for the Fourth Amendment. *See, e.g.,* Olmstead v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting) ("Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.").

> Moreover, "in the application of a constitution, our contemplation cannot be only of what has been but of what may be." The progress of science in furnishing the Government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions. "That places the liberty of every man in the hands of every petty officer" was said by James Otis of much lesser intrusions than these.

*Id.* at 474; *see* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths & the Case for Caution*, 102 MICH L. REV. 801, 805 (2004) (noting as somewhat problematic the "popular view" that the courts should play a more aggressive role than the legislature in addressing rapidly changing technology). "When technology threatens privacy, the thinking goes, the courts and the Constiin time"[4] reveal the struggle of the Bill of Rights to adapt to an ever-advancing technological culture within the express language of each Amendment.[5]

---

tution should offer the primary response. While Congress and state legislatures may have a limited role regulating government investigations involving new technologies, the real work must be done by judicial interpretations of the Fourth Amendment." *Id.* at 802. *See generally* Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869 (1996).

[4] The phrase "switches in time" is usually used to denote a dramatic shift in American culture, either gradual or instantaneous, that significantly impacts legal jurisprudence in a manner that can be directly attributed to a certain trend or event. A good example of the "switch in time" is the effect that the Great Depression had on the United States Supreme Court's interpretation of the Commerce Clause and other parts of the Constitution. *See, e.g.*, David A. Super, *Rethinking Fiscal Federalism*, 118 HARV. L. REV. 2544, 2563 (2005) ("After 1937, the Court essentially abandoned attempts to enforce a constitutional division of functions that constrained Congress's ability to regulate in areas of traditional 'local concern.'"). In the modern era, both gradual (relatively speaking) and dramatic shifts in time include rapid advances in technology and monitoring and search capabilities by the government, as well as the events of September 11, 2001, which set in motion a crucial and ongoing effort to balance rights and freedoms with safety and order. *See, e.g.*, John M. Burkoff, *"A Flame of Fire": The Fourth Amendment in Perilous Times*, 74 MISS. L.J. 631 (2004).

> We *can* do this. We *can* respect individual rights and we *can* protect ourselves, at the very same time, from the awful threats that now face us.
>
> Indeed, not only *can* we do this, it is, as Americans, just precisely what we *must* do. We must keep the balance true, we must keep the constitutional fire aflame even, *perhaps especially*, in perilous times.

*Id.* at 680; David A. Sklansky, *Back to the Future:* Kyllo, Katz, *and Common Law*, 72 MISS. L.J. 143, 143-44 (2002) ("Recently these questions have become more pressing. The atrocities of September 11, 2001, along with many of the law enforcement measures taken in response, have properly prompted wide reconsideration of the appropriate balance between liberty and security in modern-day America."); *see also* AMITAI ETZIONI, HOW PATRIOTIC IS THE PATRIOT ACT, FREEDOM VERSUS SECURITY IN THE AGE OF TERRORISM 1 (2004) ("[T]he starting point of any reasonable deliberation about our national security is the recognition that we face two profound commitments: protecting our homeland and safeguarding our rights."); David A. Sklansky, *Police and Democracy*, 103 MICH. L. REV. 1699, 1702 (2005) ("As for the trade-offs, we sometimes talk as though effective policing is like trains running on time: something we need to sacrifice a little if we wish to live in a democracy. The goal is to strike the right balance between letting the police do their job and preserving our democratic liberties.").

[5] Recently, my mother, a computer science professor at Georgia Tech, mentioned that computer science students are now required to complete "CS 4001D *Computing, Society, & Professionalism.*" Interestingly, at the same time lawyers,

From the outset, I must admit that perpetrators convicted of sexually abusing, exploiting or victimizing children disgust me.[6] As this is the case, considering, researching, discussing

---

attuned to the world of arguments instead of answers, attempt to deal with the information and Internet age from a legal standpoint, computer science students and professionals face a similar challenge to understand esoteric notions of ethics, including feminine ethics, law, privacy, utilitarianism, and consequentialism. The title of the course text, SARA BAASE, A GIFT OF FIRE (2d ed. 2002), is a somewhat telling allusion to the widespread advantages and detriments of modern technology. The struggle to keep sight of the text of the Fourth Amendment in the context of emerging technology is certainly not new. *See* Katz v. United States, 389 U.S. 347, 364-65 (1967) (Black, J., dissenting) (emphasis added).

> My basic objection is twofold: (1) I do not believe that the words of the Amendment will bear the meaning given them by today's decision, and (2) *I do not believe that it is the proper role of this Court to rewrite the Amendment in order "to bring it into harmony with the times" and thus reach a result that maybe people believe to be desirable.*
>
> While I realize that an argument based on the meaning of words lacks the scope, and no doubt the appeal, of broad policy discussions and philosophical discourses on such nebulous subjects as privacy, for me the language of the Amendment is the crucial place to look in construing a written document such as our Constitution.

*Id.* (emphasis added). "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." Kyllo v. United States, 533 U.S. 27, 33-34 (2001); *see also* United States v. Kincade, 379 F.3d 813, 821 (9th Cir. 2004).

> The freedoms established in the Bill of Rights—including the Fourth Amendment right to be free from unreasonable governmental searches and seizures—were meant to endure. Advances in science and technology recurrently exert pressure on the scope and meaning of the Fourth Amendment, but the privacy and security protected by the Fourth Amendment should not depend on innovations in technology.

Tracey Maclin, Katz, Kyllo, *and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51, 51 (2002). *See also* James J. Tomkovicz, *Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures*, 72 MISS. L.J. 317, 317-18 (2002) ("The notion that technological developments are mixed blessings is hardly a novel or recent revelation. Others have observed that the enhancements of human abilities afforded by innovative technologies are quite typically swords with two very sharp edges.").

[6] Particularly disturbing is the manner in which the Internet has acted to normalize deviant sexual activity with children in the warped minds of offenders. Specifically, the Internet has the effect of lowering offenders' inhibitions and their belief that their behavior violates cultural taboos.

The following quote was taken from a pedophilic web site: "*The exagger-*

---

> *ated statistics and lies about the extent of child pornography on the Internet has been the Trojan horse to suspend privacy rights and the freedom of speech for everyone. Sexually sick moral crusaders and totalitarian authorities have defined children's bodies as obscene. They aren't!*"
>
> Distorted views like the one above have become commonplace in bulletin boards, chat rooms, and on personal and organization child pornography web sites. Twenty years ago people holding such beliefs were hard pressed to locate others with similar views. Today, in a few minutes on the Internet, they can find reaffirmation of their beliefs, no matter how unhealthy, immoral, or destructive they may be. Pedophiles can easily find confirmation that child pornography and adult-child sex is not immoral, is not harmful to children, and is not government's business.

Sen. Joseph L. Bruno, Majority Leader, *Child Pornography, Prostitution and Predators: Has the Internet Placed Our Children at Risk?—A Report by the New York State Senate Majority*, at 13 (2003); *see also* Victor Cline, *Witness Statement to the Commission on Child Online Protection*, San Jose State Univ., Aug. 3, 2000.

> Child pornography is particularly pernicious because the child victims (whether sexually abused while being photographed, or exposed to it as part of their seduction) are relatively powerless (due to their young age and immaturity) as well as not fully understanding the harmful potential. Their frequent willingness to trust an older person who appears to be kind and accepting of them makes more easy prey.

*Id.* at 2. I like the novel punishment mentioned by Circuit Court Judge Dorothy M. Baker (Multnomah Co., OR) in apparent "frustration and [legitimate] hostility towards child molesters: 'One time, I thought of dyeing all [child molesters] green and telling children to stay away from green people.'" Jon A. Brilliant, Note, *The Modern Day Scarlet Letter: A Critical Analysis of Modern Probation Conditions*, 1989 DUKE L.J. 1357, 1366 (1989). For my purposes, I will adopt Ken Lanning's definition of child pornography as "any visual or print medium depicting sexually explicit conduct involving a child." Kenneth V. Lanning, *Collectors*, *in*, CHILD PORNOGRAPHY AND SEX RINGS 83 (Ann Wolbert Burgess ed., 1984); *see also* William R. Graham, Jr., Comment, *Uncovering and Eliminating Child Pornography Rings on the Internet: Issues Regarding and Avenues Facilitating Law Enforcement's Access to 'Wonderland,'* 2000 MICH. ST. L. REV. 457, 459 (2000) ("[Child pornography] is associated with violence against children in two significant ways. The primary harm, is, of course, the actual sexual abuse of the children depicted in the making of the pornography. The secondary harm, however, though not as immediately evident, is just as horrific."); *see also* United States v. Yuknavich, 419 F.3d 1302 (11th Cir. 2005).

> It goes without saying that possession of child pornography is not a victimless crime. A child somewhere was used to produce the images downloaded by [Defendant], in large part, because individuals like [Defendant] exist to download the images. "Sex offenders are a serious threat in this Nation . . . . States thus have a vital interest in rehabilitating convicted sex offenders."

or even defending their "rights" is a task I must approach from an academic standpoint, constantly reminding myself that all constitutional rights have aggregate and interrelated value.[7] Ironically, I spend a great deal of time and energy exploring the rights of people I could personally care less about. Sound familiar?[8]

This article will address the specific question: what effect does the Fourth Amendment have on government actors who wish to "search"[9] the computer of a probationer convicted of producing, viewing, possessing or trafficking Internet-related

---

*Id.* at 1310 (quoting McKune v. Lile, 536 U.S. 24, 32-33 (2002)).

[7] *See, e.g.*, Skinner v. Ry. Labor Executive Ass'n, 489 U.S. 602, 650 (1989) (Marshall, J., dissenting).

> But constitutional rights have their consequences, and one is that efforts to maximize the public welfare, no matter how well intentioned, must always be pursued within constitutional boundaries. Were the police freed from the constraints of the Fourth Amendment for just one day to seek out evidence of criminal wrongdoing, the resulting convictions and incarcerations would probably prevent thousands of fatalities. Our refusal to tolerate this specter reflects our shared belief that even beneficent governmental power—whether exercised to save money, save lives, or make the trains run on time—must always yield to a "resolute loyalty to constitutional safeguards." The Constitution demands no less loyalty here.

*Id.* (citation omitted). I adopted this idea of assigning aggregate importance to Fourth Amendment principles related to intrusions that might appear *de minimus* to the public-at-large from Scott Sundby. *See* Scott E. Sundby, *Protecting the Citizen "Whilst He is Quiet": Suspicionless Searches, "Special Needs" and General Warrants*, 74 MISS. L.J. 501, 504 (2004).

[8] It should. With regards to considering and defending ideas with which we do not agree, see Burton Caine, *"The Liberal Agenda": Biblical Values and the First Amendment*, 14 TOURO L. REV. 129, 147 (1997) ("Justice Cardozo understood the necessity for defending speech 'that we hate': "Aglow even yet, after the cooling time of a century or more, is the coal from the fire that was the mind of Voltaire: 'I do not believe in a word you say, but I will defend to the death your right to say it.'") (citations omitted); *see also* United States v. Schwimmer, 279 U.S. 644, 654-55 (1929) (Holmes, J., dissenting) ("[I]f there is any principle of the Constitution that more imperatively calls for attachment than any other it is the principle of free thought—not free thought for those who agree with us but freedom for the thought that we hate.").

[9] I am using the term "search" generally at this juncture—"search" will encompass discussion and analysis that will distinguish between search and seizure and computer searches and computer monitoring.

child pornography?[10] It further explores how the resulting analysis fits into the larger Fourth Amendment jurisprudence and provides information related to the legal background and practical application of computer monitoring of probationers.

This article makes the assumption that when the government searches and/or monitors a probationer's computer, the protections of the Fourth Amendment are relevant and analysis under the Fourth Amendment becomes necessary.[11] Next, this article seeks to determine whether the protections of the Fourth Amendment have been validly "waived" in the context of a probation condition. It further examines the rationales between the two landmark United States Supreme Court decisions related to warrantless searches of probationers, attempts to explain the correlation and intersection of these two cases, and decipher the resulting Fourth Amendment legal framework which exists and acts to impact the manner in which the government can search and/or monitor Internet usage of probationers with a conviction for Internet-related child pornography.

The article can be summed up in three primary steps:

---

[10] *See generally Sex Offenders and the Internet*, SPECIAL NEEDS OFFENDERS BULLETIN, No. 3, Sept. 1998, at 16 (indicating early recognition by federal probation authorities of the challenges the Internet poses to the supervision of child-sex offenders on probation). Probation computer monitoring is notably distinct from other technology-based search and surveillance types of cases (*e.g.*, thermal imaging, pen-registers, wiretaps, etc.) in that most Fourth Amendment cases involve the gathering of information and/or evidence through serendipitous methods. This is not necessarily the case with the monitoring (or, in some cases, searching) of probationers' computers. In the vast majority of cases, probationers are clearly told that their computers will be searched and/or monitored. This is because the goal is not only detection, but deterrence. For example, the Court, in *Katz v. United States*, 389 U.S. 347, 358 n.22 (1967) stated, "'the usefulness of electronic surveillance depends on lack of notice to the suspect.'" (citation omitted). This is not the norm in computer monitoring of probationers as they have previously agreed to be "searched" in the first place.

[11] *See infra* Parts IV, V, & VI and accompanying text (discussing applicability of Fourth Amendment). *But see infra* Part X (for information on severe restrictions and deprivations of computer use by probationers that are relevant, but do not directly invoke the Fourth Amendment as there is not "search" or "seizure" and the conditions are reviewed for "reasonableness" in accordance with probation statute and not the Fourth Amendment).

Assuming that probationer has some level of protection under the Fourth Amendment:[12] (1) have these constitutional protections been waived; (2) if the protections have not been waived, what limitations does the Fourth Amendment place on this type of government intrusion; and (3) how does this type of probationary searching and/or monitoring fit into a historical perspective of Fourth Amendment jurisprudence? The remaining parts provide practical and background information to supplement the Fourth Amendment analysis with an eye towards "real-world" application.

Part I discusses the scope and certain assumptions I must make in proceeding with my overall analysis. Part II provides an overview of probation as a legal and constitutionally-relevant status and the manner in which this status acts to diminish or extinguish certain individual rights. Part III examines the role of "consent" and "waiver" in relation to the overall Fourth Amendment analysis. Part IV provides a general overview of the legal framework of warrantless searches of probationers and sets forth two separate "tracks," or bases for Fourth Amendment analysis. Part V discusses Track 1—the general "reasonableness" test applied to determine the constitutionality of a child-sex-offender computer search and/or monitoring. Part VI discusses Track 2—the Fourth Amendment exception ("special needs") analysis as relevant to child-sex-offender computer searches and/or monitoring. Part VII examines this type of search and/or monitoring in the historical context of the Fourth Amendment, specifically whether this type of computer search and/or monitoring is analogous to the traditionally-suspect "general warrant" or "writ of assistance." Part VIII discusses a mandatory application of the "Warrant-Preference" Model when the search intrudes upon the home, regardless of how diminished the occupant's reasonable expectation of privacy where obtaining the warrant would not be "impracticable." Part IX provides an overview of the manner in which the government is implementing computer monitoring as a condition of probation for relevant offenders. Finally, Part X details caselaw relevant to the circuit split which exists with regards to outright deprivation or severe limitation on Internet access generally as a condition of probation.

---

[12] *See infra* Part V.

## PART I. VARIABLES & SCOPE

### *i. Variables*

There is a constant and several variables which become important to the following discussion and analysis. In order to establish the relevant scope of this article, I have to distinguish, at the outset, among many of the possible variables that can exist when the government seeks to search[13] a probationer's computer.

The constant is that there is an individual who is on probation related to a conviction for producing, viewing, possessing or trafficking Internet-related child pornography and the computer at issue is located inside the offender's home.[14] This

---

[13] *See supra* note 9 and accompanying text.

[14] The protections of the Fourth Amendment are at their most potent when the government must enter an individual's home to search. *See* Silverman v. United States, 365 U.S. 505, 511-12 (1961) ("The Fourth Amendment, and the personal rights which it secures, have a long history. At the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.") (citation omitted).

> A man can still control a small part of his environment, his house; he can retreat thence from outsiders, secure in the knowledge that they cannot get at him without disobeying the Constitution. That is still a sizable hunk of liberty—worth protecting from encroachment. A sane, decent, civilized society must provide some such oasis, some shelter from public scrutiny, some insulated enclosure, some enclave, some inviolate place which is a man's castle.

*Id.* at 511-12 n.4 (quoting United States v. On Lee, 193 F.2d 306, 315-16 (2d Cir. 1951) (Frank, J., dissenting)); *see* Steagald v. United States, 451 U.S. 204 (1981) (strongly re-affirming that the pinnacle of Fourth Amendment protections exist when the government wishes to search a private home); Pub. Utils. Comm'n v. Pollak, 343 U.S. 451, 464 (1952) ("However complete his right of privacy may be at home, it is substantially limited by the rights of others when its possessor travels on a public thoroughfare or rides in a public conveyance."); *see also* Camara v. Mun. Court of San Francisco, 387 U.S. 523, 530-31 (1967) ("For instance, even the constant becomes relevant in distinguishing the analysis, not between the two fact-patterns[15] but between warrantless probationary searches and/or monitoring generally, and those involving probationers with a conviction for Internet-related child pornography.

The variables involve the following: (1) what type of government agency is searching the probationer's computer; (2) how do they plan to use the information or evidence they find; and (3) what type of suspicion did they have at the time they initiated the warrantless search?

### *ii. Scope*

This article requires me to establish two general fact patterns in order to proceed.[16]

(1) **Agents or officers of a governmental law enforcement agency,[17] based on at least reason-**

---

most law-abiding citizen has a very tangible interest in limiting the circumstances under which the *sanctity of his home* may be broken by official authority. . . .") (emphasis added). *But see Steagald*, 451 U.S. at 229-30 (Rehnquist, J., dissenting).

> The basic error in the Court's treatment of the common law is its reliance on the adage that "a man's home is his castle." Though there is undoubtedly early case support for this in the common law, it cannot be accepted as an uncritical statement of black letter law which answers all questions in this area. William Pitt, when he was Prime Minister of England, used it with telling effect in a speech on the floor of the House of Commons; but parliamentary speaking ability and analytical legal ability ought not to be equated with one another.

*Id.*

[15] *See infra* Part ii.

[16] Admittedly and obviously, there are numerous other fact patterns that could be relevant for analysis. I focus here, for purposes of clarity and comparison, on what I consider to be the basic fact patterns necessary for my inquiry.

[17] This could be either a probation agency or another type of law enforcement agency, but, not a strictly administrative agency which may possess quasi law enforcement powers. In *Camara v. Municipal Court of San Francisco*, 387 U.S. 523, 530 (1967), the Court recognized that while "a routine inspection of the physical condition of private property is a less hostile intrusion than the typical policeman's search for the fruits and instrumentalities of crime."

> [E]ven the most law-abiding citizen has a very tangible interest in lim-

**able suspicion,[18] enter such a probationer's home, for the purpose of searching his/her computer to discover evidence of criminal activity to be used against the offender in a criminal proceeding to obtain a subsequent conviction (hereinafter "FP1");**

**Note on FP1**: This hypothetical most closely resembles *United States v. Knights*, where the Court found that the sheriff's deputy conducting the search of Mark James Knight's (a probationer) apartment was doing so with a "reasonable suspicion" level of individualized suspicion.[19] "Reasonable suspicion" is a lower standard than probable cause. The law enforcement agency involved was attempting to discover evidence to be used in a criminal prosecution of a new crime.[20]

(2) **Agents or officers of a probation department, without any level of individualized suspicion, and pursuant to an express probation condition set forth by a court of competent jurisdiction enter such a probationer's home, for the purpose of searching/monitoring his or her computer to discover evidence or information related to whether the offender is complying with his or her conditions of probation or supervised release (hereinafter "FP2").[21]**

---

> iting the circumstances under which the sanctity of his home may be broken by official authority, for the possibility of criminal entry under the guise of official sanction is a serious threat to personal and family security.

*Id.* at 530-31.

[18] *See* United States v. Yuknavitch, 419 F.3d 1302, 1311 (11th Cir. 2005) (providing exhaustive detail as to the applicable "reasonable suspicion" standard).

[19] United States v. Knights, 534 U.S. 112, 121-22 (2001).

[20] *Id.* at 114-15.

[21] *See* Griffin v. Wisconsin, 483 U.S. 868, 885 (1987) (Blackmun, J., dissent-

**Note on FP2**: In this hypothetical, agents of a probation agency, acting on more of a supervisory than investigatory basis, monitor or search an offender's computer as part of their normal course of duties.[22] This may be with specific information about the offender or may be merely as part of a scheduled home-visit. The probation agency involved is gathering information primarily to determine whether the offender is complying with the terms of probation. Additionally, it is important to remember that the overall scope and intended aim of the probation searching and/or monitoring is conceptually different from a

---

ing). Although the discussion here is for comparison purposes, it appears relatively clear generally that searches that are part of ordinary home visits will be upheld absent extreme circumstances. *Id.* "The search in this case was not the result of an ordinary home visit by petitioner's probation agent for which no warrant is required." *Id.*

[22] *See* NICHOLAS N. KITTRIE ET AL., SENTENCING, SANCTIONS, AND CORRECTIONS: FEDERAL AND STATE LAW, POLICY, AND PRACTICE 1008 (2d ed. 2002)

> Seeing the parolee at home is a time-honored method of checking tips and maintaining contact. About one fourth of the parole officers interviewed believed in dropping in at parolee's home without prior notice. The others preferred to tell the parolee when they were coming, either specifically or perhaps "some evening next week" or "some Tuesday evening soon." The unexpected visit can be considered good surveillance because the parole officer may catch the parolee at home when he is supposed to be working or going to school. The parole officer may [even], in some states, search the premises for weapons, drugs, or other evidence of criminal activity. One of the parole officers we interviewed collects urine samples during surprise home visits if they have reason to believe that there may be a violation of parole.
>
> If the parolee is not at home his mother, father, wife or girl friend may give the parole officer some useful information. Parole officers gave us numerous examples of relatives who reported incidents showing that the parolee was getting into trouble. Some relatives will do this in an effort to keep the offender from new crimes; others will lie or cover up for him. The more positive home visits are those when the parole officer and parolee have a chance to discuss progress and problems. And if family members are present the parole officer gets some understanding of relationships in the home that may be good or bad for the parolee.

*Id.* (discussing in context of parole but very similar to home-visit in probation context).

search for evidence of a particular crime to be introduced at a criminal trial. In the course of conducting a home visit generally or computer monitoring specifically, the scope of what the probation officers can look at will be almost limitless.[23] As such, anything that they see will be in plain view.[24] Upon viewing contraband or evidence of the new crime the probation officer will likely take two distinct steps: (1) call the police so that they can charge the individual with the new crime; (the police will probably use the testimonial evidence from the probation officer to establish probable cause); and (2) take appropriate measures to revoke the offenders' probation based on the fact that the evidence constitutes a violation of the offender's probation. There is an important distinction between probation officers working with the police to search a residence where some level of individualized suspicion exists at the time the search is initiated (FP1) and probation officers discovering evidence during a rou-

---

[23] Part of the reason the "scope" of home-visits and monitoring protocols is so broad is that the probation officer is looking for more than evidence of a specific crime. For example, there may be items that, if in possession of a regular citizen, would not be contraband but for the purposes of probation conditions are forbidden. To illustrate, there is certainly nothing illegal about subscribing or possessing *MAXIM Magazine*. If the police (through a search warrant or in "plain view" in some collateral situation) found a copy at my house, they couldn't arrest me or do anything to me. However, if the same magazine is found by a probation officer in the possession of a probationer, and such a magazine violates the terms of that individual's probation, that probation could be revoked. Men's Magazine prompts Florida Sex Offender Arrest, AP, CNN.com, *at* http://www.cnn.com/2005/LAW/07/18/adult.reading.material.ap) (last visited July 2, 2005) ("Authorities in Florida are sending convicted sex offenders to jail for violating the terms of their probation by having men's magazines such as Maxim."). "In another case, sex offender Joseph Conte, 56, was arrested when the authorities found a copy of a sex manual in a drawer next to the bed the former schoolteacher shares with his wife." *Id.*

[24] *See, e.g.,* Coolidge v. New Hampshire, 403 U.S. 443, 466-67 (1971); Horton v. California, 496 U.S. 128, 133-37 (1990) (cases discussing doctrine generally and specifics of "immediately apparent" requirement); Minnesota v. Dickerson, 508 U.S. 366, 374-79 (1993); Arizona v. Hicks, 480 U.S. 321, 325-29 (1987); Texas v. Brown, 460 U.S. 730, 736-43 (1983).

> tine monitoring/home visit/inspection, performed as part of the normal course of probation and not with any specific individualized suspicion prior to the search,[25] and turning it over to law enforcement for prosecution in criminal court of a new crime.[26] However, *Knights* generally diminished the effectiveness of any defense based on the primary purpose of the law enforcement agency.[27]

Although it leads to some redundancy, I will discuss both factual situations in sections V and VI, *infra*, related to the two overall Fourth Amendment doctrines at play: special needs and reasonableness.

## PART II. PROBATION AS A LEGAL STATUS

The concept of denying individual rights to probationers[28] is hardly unique to the privacy[29] rights couched in the

---

[25] *See supra* Part I(ii)(2) (relevant fact pattern).

[26] Admittedly, certain states' probation officers have both supervisory and arrest powers. For present purposes, I distinguish probation officers and police depending on the *primary* purpose of their duties. *See also* United States v. Brown, 346 F.3d 808, 810-11 (8th Cir. 2004).

> Relying upon *United States v. McFarland*, [Defendant] argues that the trial judge should have suppressed the evidence because the probationary search was no more than a "rule for police investigation." Stated differently, he argues that [the probation officer] was only a "stalking horse" for law enforcement. The government counterargues that *United States v. Knights* eliminates this stalking horse theory. We agree with the government.
>
> **i. Probationary Searches**
>
> In *McFarland*, we "agree[d] that a parole search is unlawful when it is nothing more than a ruse for police investigation." We also noted that parole officers may work with police officers provided the parole officers are pursuing parole-related objectives. But, the *Knights* case teaches that traditional Fourth Amendment analysis—not official purpose—determines whether a probationary search is constitutional.

*Id.* (citations omitted).

[27] *Id.*

[28] *See* Devon A. Corneal, Comment, *Limiting the Right to Procreate:* State v. Oakley *and the Need for Strict Scrutiny of Probation Conditions*, 33 SETON HALL L. REV. 447, 455 (2003).

Fourth Amendment.[30] For example, thirty-one states prohibit

---

> Surprisingly, the American probationary system began, not with a legislative enactment, but with the actions of a cobbler. Probation in the United States first started when John Augustus convinced the Boston Police Court to release a drunk to his custody rather than to jail him. In his lifetime, Augustus arranged the bail of nearly 2,000 defendants, and earned the titles of "inventor" and "father" of probation. Augustus's *ad hoc* system ended in 1878 when Massachusetts passed the first probation statute; other states and the federal government followed suit. Today, probation statutes affect millions of individuals.

*Id.*

[29] *See supra* note 1 and accompanying text.

[30] *See* Brief of the Criminal Justice Legal Foundation as Amicus Curiae Supporting Petitioner, United States v. Knights, 534 U.S. 112 (2001) ("Public safety is the Achilles' heel of any probation system. While society can reap substantial benefits from this less costly and more rehabilitative alternative to prison, having convicted criminals serve their sentence in society gambles with public safety. A probation system that cannot protect will lose support."). There is a marked distinction between an examination of the express "right of privacy" created by the Fourth Amendment and the misinterpretations that have resulted in a long line of "penumbral privacy rights" and unenumerated "fundamental" rights.

> [T]he key to discovering whether [a right] is "fundamental" is not to be found in comparisons of the relative societal significance of education as opposed to subsistence or housing. Nor is it to be found by weighing whether education is as important as the right to travel. Rather, the answer lies in asserting whether there is a right to education *explicitly or implicitly guaranteed by the Constitution.*

San Antonio Indep. Sch. Dist. v. Rodriguez, 411 U.S. 1, 33-34 (1973) (emphasis added). *See, e.g.,* Zablocki v. Redhail, 434 U.S. 374, 383 (1978) (marriage); Carey v. Population Servs. Int'l, 431 U.S. 678, 684-85 (1977) (contraception); Eisenstadt v. Baird, 405 U.S. 438, 453-54 (1972) (procreation); Loving v. Virginia, 388 U.S. 1, 12 (1967) (marriage); Griswold v. Connecticut, 381 U.S. 479, 484-86 (1965) (procreation); Prince v. Massachusetts, 321 U.S. 158, 166 (1944) (family relationships); Skinner v. Oklahoma, 316 U.S. 535, 541-42 (1942) (contraception); Pierce v. Soc'y of Sisters, 268 U.S. 510, 535 (1925) (child rearing and education); *see also* Katz v. United States, 389 U.S. 347, 350 (1967) ("[T]he Fourth Amendment cannot be translated into a general constitutional 'right to privacy.'"). I disagree, in concept, practice, and application with the idea that both "explicit" and "implicit" "guarantees" found (or *discovered*, I guess) in the text of the Constitution (assuming that there is any validity, at all, to the idea of *implicit* commands or "guarantees" in a written document) are somehow afforded equal weight in quashing the intentions set forth by legitimate acts of democratic government such as those found in the cases above. If notions of "drafter's intent" or *expressio unius est exclusion alterius* have any validity, (and I think they do) the fact that the Framers explicitly set forth "privacy" rights in the Third and Fourth Amendments discredits the idea that it was their simultaneous intention to set forth a general "penumbral" right of felons from voting while they are on probation[31] and a major-

---

privacy without any mention of it at all. A full discussion of the disturbing trend blurring the lines between penumbral privacy, substantive due process, and rights couched as "liberty" which elude any and all legitimate aims of democratic government is outside the scope of this article. However, because the analysis set forth herein is, in large part, contingent on the fact that the computer at issue is located in the probationer's house, some discussion of this trend of judicial creationism becomes necessary. A particularly disturbing example of "judicial creationism" can be found in the Court's holding in *Lawrence v. Texas*, 539 U.S. 558, 562 (2003), authored by Justice Kennedy:

> Liberty protects the person from unwarranted government intrusions into a dwelling or other private places. *In our tradition the State is not omnipresent in the home*. And there are other spheres of our lives and existence, *outside the home*, where the State should not be a dominant presence. Freedom extends beyond spatial bounds. Liberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct. The instant case involves liberty of the person both in it spatial and more transcendent dimensions.

*Id.* (emphasis added). While this type of "liberty," personal "autonomy," and privacy may be desirable, or perhaps even increasingly necessary with advances in technology and the ability of the government to collect and warehouse information about all aspects of our lives, if this type of "spatial" or transcendental liberty is to emerge, it should be after full and robust debate by the people (in the form of an Amendment or other applicable democratic assertion) and not at the whim of at least five lawyers with life terms. Justice Kennedy's prose, while somewhat eloquent, is misplaced in the context of interpreting a static Constitution. *See* David A. Anderson, *Metaphorical Scholarship*, 79 CAL. L. REV. 1205, 1214-15 (1991) (reviewing STEVEN H. SHIFFAIN, THE FIRST AMENDMENT, DEMOCRACY, AND ROMANCE (1990)) ("[Metaphor] liberates the author from some of the rigidity of exposition, but also from the demands of precision and clarity. The subtlety that makes the poet's boon can be the lawyer's bane . . . ."). Perhaps this type of spatial zone of liberty and privacy should be the next step of an evolving nation. The question is not, *should the United States evolve?* The question is: *are the courts or the legislature the proper means of this "evolution"?*

> There is plenty of room within this system for "evolving standards of decency" but the instrument of evolution—or, if you are more tolerant of the Court's approach, the herald that evolution has occurred—is not the nine lawyers who sit on the Supreme Court of the United States, but the Congress of the United States and the legislatures of the fifty states . . . .

Antonin Scalia, Associate Justice, United States Supreme Court, from remarks given at a conference by the Pew Forum on Religion and Public Life at the University of Chicago Divinity School, http://pewforum.org/deathpenalty/resources/transcript3.php3 (last visited Oct. 8, 2005); *see also* Planned Parenthood v. Casey, 505 U.S. 833, 989-90 (1992) (Scalia, J., dissenting) ("It is difficult to maintain the ity of states prohibit probationers from owning or possessing a firearm[32] or associating with certain people and groups of people.[33] Other restrictions blur the line between constitutional rights and basic human rights or expectations such as procreation and marriage.[34]

Simply put, an individual on probation is not "free" and "do[es] not enjoy 'the absolute liberty to which every citizen is entitled, but only . . . conditional liberty properly dependent on observance of special [probation] restrictions.'"[35] Then why

---

illusion that we are interpreting a Constitution rather than inventing one, when we amend its provisions so breezily.").

[31] *See* The Sentencing Project *Felony Disenfranchisement Laws in the United States*, *at* http://www.sentencingproject.org/pub_D5.cfm (last visited June 27, 2005).

[32] U.S. CONST. amend. II.

[33] U.S. CONST. amend. I.

[34] *See* Jennifer Levi, *Probation Restrictions Impacting the Right to Procreate: the Oakley Error*, 26 W. NEW ENG. L. REV. 81, 82 (2004) (detailing 4-3 ruling by state court upholding a probation condition restricting probationer's right to have children as constitutional.); Shana Weiss, *A Penny For Your Thoughts: Revisiting* Commonwealth v. Power, 17 LOY. L.A. ENT. L. REV. 201, 202-03 (1996) (generally discussing different types of probation restrictions which interfere with varying levels of civil and constitutional rights); Steven S. Spitz, *The Norplant Debate: Birth Control or Woman Control*, 25 COLUM. HUM. RTS. L. REV. 131 (1993) (discussing compulsory use of Norplant contraceptive by courts as condition for female probationers); *see also* Rebecca L. Miles, *Criminal Consequences for Making Babies: Probation Conditions that Restrict Procreation*, 59 WASH. & LEE L. REV. 1545 (2002) (interesting contextual argument related to the distinction between punishing individuals for their past actions versus punishing them by restricting ability to make future choices on fundamental, personal matters).

> When people make irresponsible choices, courts customarily hold them accountable for their actions through civil or criminal sanctions. However, occasionally courts punish criminal defendants who have made irresponsible choices by removing or restricting their ability to choose again. Operating pursuant to probation statutes, courts occasionally have burdened probation sentences with conditions that restrict probationers' most personal decisionmaking.

*Id.* at 1545-46; *see also* Dorothy E. Roberts, *Punishing Drug Addicts Who Have Babies: Women of Color, Equality, and the Right of Privacy*, 104 HARV. L. REV. 1419 (1991) (discussing role of constitutional, privacy and human rights in context of procreation rights).

[35] Griffin v. Wisconsin, 483 U.S. 868, 874 (1987) (quoting Morrissey v. Brewer, 408 U.S. 471, 480 (1972)); *see also* United States v. Knights, 534 U.S. 112, 119 (2001) ("Just as other punishments for criminal convictions curtail an offender's freedoms, a court granting probation may impose reasonable conditions that deprive

is such a thorough analysis of the relationship between the Fourth Amendment and searches involving probationers necessary? The primary reason stems from the fact that when other types of probation conditions are not followed, the governmental action involves only the probation department and any punitive[36] action is purely administrative (i.e., a revocation of probation). The Supreme Court has traditionally given wide deference to this type of administrative proceeding. Further, the Court has held that the exclusionary rule is not applicable and evidence collected in violation of the Fourth Amendment is admissible for purposes of parole revocation hearings, and the majority of reviewing courts, both state and federal, have extended this doctrine to probation revocation hearings.[37]

---

the offender of some freedoms enjoyed by law-abiding citizens.").

[36] Punitive in this context being something that is detrimental to the probationer generally. As revocation of probation does not amount to additional "jeopardy" it is not truly punitive in legal or double jeopardy sense. *See* U.S. CONST. amend. V.

[37] *See* Pennsylvania Bd. of Probation & Parole, 524 U.S. 357, 369 (1998) (emphasis added) (citations omitted).

> We have long been averse to imposing federal requirements upon the parole systems of the States. A federal requirement that parole boards apply the exclusionary rule, which is itself a "grud[g]ingly taken medicament," would severely disrupt the traditionally informal administrative process of parole revocation. The marginal deterrence of unreasonable searches and seizures is insufficient to justify such an intrusion.

*Id.* (citations omitted); *see also* 77 A.L.R. 3d 636 § 2:

> These courts have looked to the purpose of the [exclusionary] rule as their guide, and in those proceedings where the exclusion of such evidence would not serve to deter illegal searches, they have felt free to allow the evidence to be used. Acting on this principle, most courts have refused to extend the exclusionary rule to probation revocation proceedings.

*Id. See, e.g.,* United States *ex rel.* Lombardino v. Heyd, 318 F. Supp. 648 (D.C. La 1970); *see also Ex parte* Caffie, 516 So. 2d 831 (Ala. Crim. 1987); Holcomb v. State, 644 So. 2d 46 (Ala. Crim. App. 1994); Chenault v. State, 777 So. 2d 314 (Ala. Crim. App. 2000); State v. Alfaro, 623 P.2d 8 (Ariz. Ct. 1980); State v. Towle, 609 P.2d 1097 (Ariz. Ct. App. 1980); McGhee v. State, 752 S.W.2d 303 (Ark. Ct. App. 1988); Harris v. State, 606 S.W.2d 93 (Ark. Ct. App. 1980); People v. Coleman, 533 P.2d 1024 (Cal. 1975); People v. Vanella, 71 Cal. Rptr. 152 (Cal. Ct. App. 1968); People v. Hayko, 86 Cal. Rptr. 726 (Cal. Ct. App. 1970); People v. Rafter, 116 Cal.

Limitations of probationers' Fourth Amendment privacies[38] are unique in the overall context of diminished rights given a probationer's legal status. If the government seeks to introduce evidence of a new crime against the individual in a judicial proceeding, and this evidence was collected unlawfully, it will be suppressed.[39] Conceptually, it is the affirmative

---

Rptr. 281 (Cal. Ct. App. 1974); People v. Fuller, 210 Cal. Rptr. 1 (Cal. Ct. App. 1983); People v. Willis, 197 Cal. Rptr. 281 (Cal. App. Dep't Super. Ct. 1983); People v. Calais, 111 Cal. Rptr. 654 (Cal. Ct. App. 1974); People v. Atencio, 525 P.2d 461 (Colo. 1974); People v. Wilkerson, 541 P.2d 896 (Colo. 1975); People v. Ressin, 620 P.2d 717 (Colo. 1980); Brill v. State, 32 So. 2d 607 (Fla. 1947); Bernhardt v. State, 288 So. 2d 490 (Fla. 1974); State *ex rel.* Ard v. Shelby, 97 So. 2d 631 (Fla. Dist. Ct. App. 1957); Singletary v. State, 290 So. 2d 116 (Fla. Dist. Ct. App. 1974); Owens v. State, 354 So. 2d 118 (Fla. Dist. Ct. App. 1978); Latham v. State, 360 So. 2d 127 (Fla. Dist. Ct. App. 1978); Kinzer v. State, 366 So. 2d 874 (Fla. Dist. Ct. App. 1979); State v. Dodd, 396 So. 2d 1205 (Fla. Dist. Ct. App. 1981); Huppertz v. State, 399 So. 2d 992 (Fla. Dist. Ct. App. 1981); Bruno v. State, 343 So. 2d 1335 (Fla. Dist. Ct. App. 1977); People v. Dowery, 312 N.E.2d 682 (Ill. App. Ct. 1974); People v. Swanks, 339 N.E.2d 469 (Ill. App. Ct. 1975); People v. Holliday, 743 N.E.2d 587 (Ill. App. Ct. 2001); Dulin v. State, 346 N.E.2d 746 (Ind. App. 1976); Tiryung v. Commonwealth, 717 S.W.2d 503 (Ky. Ct. App. 1986); State v. Caron, 334 A.2d 495 (Me. 1975); Chase v. State, 522 A.2d 1348 (Md. 1987); Commonwealth v. Olsen, 541 N.E.2d 1003 (Mass. 1989); People v. Perry, 505 N.W.2d 909 (Mich. App. 1993); State v. Martin, 595 N.W.2d 214 (Minn. Ct. App. 1999); State v. Thorsness, 528 P.2d 692 (Mont. 1974); Stone v. Shea, 304 A.2d 647 (N.H. 1973); State v. Field, 571 A.2d 1276 (N.H. 1990); State *ex rel.* Corgan v. King, 868 P.2d 743 (Okla. Crim. App. 1994); State v. Ray, 598 P.2d 1293 (Or. Ct. App. 1979); Commonwealth v. Davis, 336 A.2d 616 (Pa. Super. Ct. 1975); State v. Spratt, 386 A.2d 1094 (R.I. 1978); Johnson v. Commonwealth, 462 S.E.2d 907 (Va. Ct. App. 1995); State v. Kuhn, 499 P.2d 49 (Wash. Ct. App. 1972). For a recent example, see, *Jones v. Superior Court*, 8 Cal. Rptr. 3d 687 (Cal. Ct. App. 2004) (holding that the exclusionary rule does not apply to a probation revocation hearing). Some jurisdictions rule that the exclusionary rule does apply to probation revocation hearings due to the belief that evidence obtained via unreasonable search and seizure should not be used for *any* purpose "imperative of judicial integrity." *See e.g.,* State v. Scarlet, 800 So. 2d 220 (Fla. 2001); State v. Marquart, 945 P.2d 1027 (N.M. Ct. App. 1997); State v. Lampman, 724 P.2d 1092 (Wash. Ct. App. 1986).

[38] *See supra* note 1 and accompanying text.

[39] *See* Weeks v. United States, 232 U.S. 383, 391-93 (1914) (suppression doctrine applied to federal authorities); Mapp v. Ohio, 367 U.S. 643, 660 (1961) ("Having once recognized that the right to privacy embodied in the Fourth Amendment is enforceable against the States, and that the right to be secure against rude invasions of privacy by state officers is, therefore constitutional in origin, we can no longer permit that right to remain an empty promise.").

action of the government to prosecute the probationer for a new crime, and the remedy which exists, that creates the primary constitutional cause of action discussed herein.[40]

## PART III. "CONSENT" AND "WAIVER"

One common, and somewhat intuitive, explanation for the right of government officials to monitor and/or search the computer of an individual with a prior child pornography conviction is simply that the probationer previously agreed to the terms of probation and has thus consented[41] to the future search[42] and has waived[43] any constitutional claims.[44]

---

[40] *But see* United States v. Lifshitz, 369 F.3d 173, 188-93 (2d Cir. 2004) (where there was no actual search and facial challenge of probation condition (prior to any application by the government against probationer) was sustained.).

[41] *See* Ferguson v. City of Charleston, 532 U.S. 67, 93 (2001) (Scalia, J., dissenting) ("It is rudimentary Fourth Amendment law that a search which has been consented to is not unreasonable.").

[42] *See supra* note 9 and accompanying text.

[43] *See generally* Daniel P. Blank, *Plea Bargain Waivers Reconsidered: A Legal Pragmatist's Guide to Loss, Abandonment and Alienation*, 68 FORDHAM L. REV. 2011 (2000).

> The doctrine of criminal waiver currently suffers under a tremendous weight of "theory-guilt." Legal scholars have struggled mightily to explain why, during the course of a criminal prosecution, the defendant may waive most, though not all, of his fundamental constitutional and statutory rights. Waiver in the disposition of criminal charges is so frequently invoked that commentators have long suggested that "[i]t is waiver of rights the permits the system of criminal justice to work at all."

*Id.*

[44] Katz v. United States, 389 U.S. 347, 358 n.22 (1967), *superseded by statute* 18 U.S.C. § 2510 (2000). The United States Supreme Court, in progressing from a property analysis to a privacy analysis with regards to the scope of the Fourth Amendment, has always been cognizant of the role of "consent" to the application of the Amendment to individuals. *Id.* at 350-51. For example, in the Court's expansive landmark ruling, *Katz v. United States*, the Court expressly stated that "[a] search to which an individual consents meets Fourth Amendment requirements." *Katz*, 389 U.S. at 358 n.22. *See* Marc R. Lewis, *Lost in Probation: Contrasting the Treatment of Probationary Search Agreements in California and Federal Courts*, 51 UCLA L. REV. 1703, 1723 (2004) ("The Supreme Court has been clear in holding that 'consent' and 'waiver' are established exceptions to the Fourth Amendment's warrant requirement. But because the concepts are inexorably linked, courts and commentators have had some difficulty distinguishing con-

Consent carries with it an important conceptual historical underpinning. If we understand the Bill of Rights, the first ten amendments to the Constitution, to be important limitations on the power of the federal government, and in so being, a grant of individual "rights to the people" and citizens of the various states, implicit and intrinsic in the grant of any "right" is an individual's power to waive it.[45] It would be a shallow concession on the part of the government to convey "rights" which are not truly at the control of the very citizenry they are meant to empower.[46]

For example, the freedom to speak does not mean one *must* speak.[47] The right to bear arms does not necessarily

---

sent from waiver. For example, consider the following sentence: '[C]onsent is a voluntary waiver of a person's Fourth Amendment rights.' While this is undoubtedly true—consent is a voluntary waiver of certain protections—using "waiver" to define "consent" reflects the fundamental confusion between the two doctrines. Accordingly . . . [the following definition provided]: [t]he language in probation agreements creates a waiver of Fourth Amendment rights whereby a probationer consents to future searches."); *see also* Schneckloth v. Bustamonte, 412 U.S. 218, 242-43 (1973) ("Nor can it even be said that a search, as opposed to an eventual trial, is somehow 'unfair' if a person consents to a search. While the Fourth and Fourteenth Amendments limit the circumstances under which the police can conduct a search, there is nothing constitutionally suspect in a person's voluntarily allowing a search. The actual conduct of the search may be precisely the same as if the police had obtained a warrant."). *See generally* Davis v. United States, 328 U.S. 582, 593-94 (1946) (early case recognizing "consent" as valid exception to both warrant and probable cause).

[45] *See* LEONARD W. LEVY, ORIGINAL INTENT AND THE FRAMERS' CONSTITUTION 146 (1988) ("The Bill of Rights did just that: it was a bill of restraints on the United States. Congress submitted those restraining amendments to the states for ratification on September 25, 1789, and the requisite number of state legislatures ratified them by December 15, 1791.").

[46] It would be either a shallow concession by the government, or a hollow victory by the people, depending on one's view of the Bill of Rights. *See* LEVY, *supra* note 45, at 146 ("The triumph of individual liberty against government power is one of our history's noblest themes, epitomized by the Bill of Rights."). *But see* United States v. Mezzanatto, 513 U.S. 196, 204 (1995) (finding that although most protections within a criminal prosecution are waivable, some may be so integral to the fact-finding process that they cannot be waived, e.g., right to conflict-free counsel); United States v. Gambino, 59 F.3d 353, 359-60 (2d Cir. 1995) (ruling consistently with every circuit that has ruled on the issue, due to the great interest in a speedy-trial, defendants cannot waive the protections of the Speedy Trial Act).

[47] *See generally* U.S. CONST. amend. I. *See, e.g.,* West Va. St. Bd. of Educ. v.

mean that I must own a gun.[48] Simply because the government cannot quarter soldiers in my home during peacetime, it does not necessarily follow that I cannot invite them in to stay, if I so choose.[49] I have a right to (non-excessive) bail, but I can certainly choose to sit in jail instead.[50] It is not clear that I can choose cruel or unusual punishment, my guess is that few have tried, but you get the point.[51]

The most crucial rights we possess as Americans are strengthened, not weakened, by the fact that we can waive or choose *not* to exercise them.[52] For example, the *Miranda*

---

Barnette, 319 U.S. 624 (1943) (case restricting government's right to "compel" speech and speech-conduct).

[48] *See generally* U.S. CONST. amend. II. A small number of communities and counties have enacted legislation that requires the head of each household to own at least one firearm with ammunition. For example, such an ordinance was passed in Kennesaw, Georgia in 1982. *See* Jonathan Hamilton & David Burch, *Gun Ownership—It's the Law in Kennesaw*, Marietta Daily (available at http://www.rense.com/general9/gunlaw.htm) (last visited July 27, 2005). *Id.* The law was passed to "protect the safety, security and general welfare of the city and its inhabitants." *Id.* After the ACLU challenged the law in federal court, the city added a "conscientious objector" exemption. *Id.*

[49] *See generally* U.S. CONST. amend. III.

[50] *See generally* U.S. CONST. amend. VIII.

[51] *Id.*

[52] *See* United States v. Drayton, 536 U.S. 194 (2002).

> In a society based on law, the concept of agreement and consent should be given a weight and dignity of its own. Police officers act in full accord with the law when they ask citizens for consent. It reinforces the rule of law for the citizen to advise the police of his or her wishes and for the police to act in reliance on that understanding. When this exchange takes place, it dispels inferences of coercion.

*Id.* at 207. *But see* Ric Simmons, *Not "Voluntary" But Still Reasonable: A New Paradigm for Understanding the Consent Searches Doctrine*, 80 IND. L.J. 773 (2005).

> So, were the actions of the government agents "reasonable" in *Drayton*? This is a question the Court never directly answered, although the Court at times wrote as though this were the question it meant to answer. Instead, the opinion keeps returning to the question of voluntariness. As a result, the Court ended up defending the search not because the search was "reasonable" (which was arguably true) but rather because the Court claimed the defendants acted "voluntarily" (which was almost certainly not true). The consequence of this misdirection was a firestorm of academic criticism and a scathing reception by the public

---

> at large. It is no exaggeration to say that the nearly unanimous condemnation of the Court's rulings on consensual searches is creating a problem of legitimacy which threatens to undermine the integrity of judicial review of police behavior. What has gone wrong?

*Id.* at 774-75. I cannot join in this "unanimous condemnation" of the Court's voluntariness rulings without accepting a type of paternalistic approach which views citizens as being helpless to interact with the police, specifically, or government, generally, to assert or waive their constitutional rights. *See supra* note 44 and accompanying text. In his article, Professor Simmons criticizes the United States Supreme Court for failing to adopt a consistent "test" that "fully comports with the real-life confrontations occurring on the street." Simmons, *supra*, at 773. This common misconception, that people, (*especially* criminals like Brown and Drayton who smuggle 483 grams and 295 grams of cocaine, respectively, *Drayton*, 536 U.S. at 199) have no "power" to assert their Fourth Amendment rights because they are so afraid of the police that it should make a constitutional difference is more misleading as to what really goes on in police-citizen encounters "on the street" than the school of thought, whether stated or unstated, that can only accept or comprehend consent in some context of coercion. It is this type of paternalism, not the actions of the police, which strip these individuals of their constitutional significance. A true "civil-libertarian," in this context, would be equally cognizant and interested in defending the collective power citizens maintain when they are free to control the destiny of their rights through assertion *or* waiver. Regardless of my conclusion as to the merits of this "school of thought" and some skepticism that any condemnation of the Court is, in fact, unanimous, (or even close to it) it seems clear that a significant academic backlash does exist towards the Court's use of voluntariness generally and the *Drayton* opinion specifically. In this "backlash" I sense three primary themes: (1) proponents seek some type of "academic street-cred" (short for credibility) by believing that the view from their ivory tower is somehow superior to the view from the High Court chambers of what really occurs "in the street"; (2) an ostensible concern for the "rights" of the "coerced" which is, in actuality, a paternalistic view of people who need to be "saved" by academics from making their own constitutional decisions; and (3) a myopic belief that police are a cure worse than the disease and societal problem of crime. *See* Arnold H. Loewy, *Cops, Cars, and Citizens: Fixing the Broken Balance*, 76 ST. JOHN'S L. REV. 535 (2002). For example, with reference to number three, above, "I do not mean to suggest that the officer is always, or even usually, lying. Those caught with drugs have a great deal of incentive to lie, *and their credibility should be at least as suspect as the police officer's.*" *Id.* at 556 (emphasis added). Also disturbing is the ongoing inability of certain academics to accept that there could be cooperation between the police and citizenry in regards to consent searches. While it may seem naïve to believe that, in a democratic society where the majority of the people *should* agree with the laws that govern them, a consent search could be "salutary" this type of consent search goes on everyday "on the street." Professor Loewy seems to doubt the very existence of the "consent-search" in the real world because he only seems to view it through the prism of those who do, in fact, have something to hide. *Id.* at 552-53.

---

> The concept of a consent search sounds salutary. The conflict between police officer and citizen is gone, and the two are working together for the common goal of creating a better society. [The scenario] . . . might look something like this:
>
> Police officer: You were going thirty-five mph in a twenty-five mph zone. We really can't have that.
>
> You: I understand officer. Thanks for calling it to my attention.
>
> Police officer: While I have you stopped do you mind if I look in the trunk of your car? You don't have to, but it would be helpful to me if you would consent.
>
> You: I don't have anything in there, but if you want to look, it's fine with me.
>
> Police officer (after viewing empty trunk): Thanks for your help. Now remember no more speeding.
>
> The problem is that the hypothesized scenario is not what typically happens. Instead, a truly voluntary consent, while perhaps not oxymoronic, certainly does not seem to be the rule, *at least according to the defendants in the litigated cases.*

*Id.* (emphasis added). Why does there have to be inevitable "conflict" between the police and the citizen? Is it impossible to believe that an innocent person could work with the police? The police officer told the occupant, "You don't have to." *Id.* at 552. Apparently, even when the occupant is told "you don't have to consent," they are somehow powerless to either assert or waive their constitutional rights. This is telling of the paternalistic view of citizenry that pervades much of the "backlash" against the *Drayton* opinion and the Court's voluntariness doctrine. *See also* Janice Nadler, *No Need to Shout: Bus Sweeps and the Psychology of Coercion*, 2002 SUP. CT. REV. 153, 222 (2002) ("If this is the determination that underlies the decision in *Drayton*, then the Court should have explicitly stated it and justified it—rather than relying on the implausible assertion that bus passengers, when they are individually confronted by armed police officers who want to search them, feel free to ignore the police or outright refuse their requests.). Here, the author counters what she considers to be implausible logic in one direction with implausible logic in the reverse direction. Following this logic, there is not *any* person who, when confronted by "armed police officers" (do Americans have any experience, at all, with unarmed police officers?) feels free to either assert their Fourth Amendment rights or exercise their rights through affirmative waiver? For example, if F. Lee Bailey and the late Johnny Cochran are traveling together by Greyhound, and are placed in the same situation as Brown and Drayton, do they similarly lack the capacity to exercise their constitutional rights? Would their waiver also be *per se* coercive because of their fear of bus-riding, gun-toting cops? I do not believe that the Court should inquire into the subjective feeling of "free[dom]" individuals have when dealing with police. This seems too far skewed towards concluding that all police-citizen encounters are coercive simply by the presence of an armed police officer. The idea that "ignorance of your rights" should invalidate a waiver of a right has no more plausibility to criminal procedure jurisprudence as the general notion that "ignorance of the law" should be a valid defense. *See generally*, David

---

S. Kaplan & Lisa Dixon, *Coerced Waiver and Coerced Consent*, 74 DENV. U. L. REV. 941 (1997); Stephen A. Saltzburg, *The Supreme Court, Criminal Procedure and Judicial Integrity*, 40 AM. CRIM. L. REV. 133 (2003). Although he would disagree with my overall conclusion, George C. Thomas, III, asks a similar question while coming to the opposite conclusion:

> I suppose it is more difficult to work up enthusiasm to protect those who are carrying almost 800 grams (twenty-seven ounces) of cocaine. After all, atheists may challenge our belief structure, but drug dealers threaten us and our children with addiction and death. Yet I cannot resist the conclusion that Drayton's "consent" is consent only in the most academic sense. Defining "consent" as the lack of overt coercion is a pretty impoverished notion when one is facing armed police who appear to be blocking egress from a bus. Given what we are learning about the reaction of citizens to civilian authority, and remembering that the ones requesting consent in drug cases are officers who carry guns and have the power to arrest, a definition of consent that includes every noncoerced act is unrealistic. Moreover, Janice Nadler raises the provocative possibility that while the police officer perceives a friendly conversation, the suspect may perceive coercion. *So whose perspective "counts"?*

George C. Thomas, III, *Time Travel, Hovercrafts, and the Framers: James Madison Sees the Future and Rewrites the Fourth Amendment*, 80 NOTRE DAME L. REV. 1451, 1510-11 (2005) (emphasis added); *see also* DAVID A. HARRIS, PROFILES IN INJUSTICE: WHY RACIAL PROFILING CANNOT WORK 34-37 (2002). Professor Harris is undoubtedly one of the preeminent experts and scholars with regards to "racial profiling." In the following passage from his book, Professor Harris concludes that, even where individuals are expressly told that they can refuse, their consent is not voluntary but instead given "because that is how people respond to authority." *Id.* at 34.

> In recently completed doctoral work, Illya Lichtenberg of Rutgers University tested the idea of the voluntariness of consent to search. Using data from Ohio and Maryland, which together included more than nine thousand consent searches, Lichtenberg's findings directly contradict the Supreme Court's assumptions. Lichtenberg found that about 90 percent of drivers who were asked for consent gave it—rates far higher than in any of the classic psychology experiments on compliance with authority. There were no significant differences in the rates of consent when the data were broken down by sex, by age, or by race. Basically, almost everyone consents; few people—just one out of ten—refuse. Even the use of a warning—telling the suspect that he or she was free to go before asking for consent—made no difference. All in all, Lichtenberg's work raises considerable doubt that these interactions can ever be considered voluntary. People who agree to searches do not make a free choice to grant consent. Rather, they consent because that is how people respond to authority. Calling such an interaction voluntary is at best misleading and at worst completely wrong.

*Id.* Again, I would reiterate my belief that, especially where people are expressly warnings, which most can likely recite verbatim (or close) from television and movies,[53] include many of the crucial individual rights Americans hold dear.[54] However, what makes them *individual rights* is, in part, the fact that the individual can choose not to assert them. For example, you do not have to remain silent; you can refuse an attorney; you can even confess.[55] Just as stupid laws are not always unconstitution-

---

told "you are free to leave—you do not have to give consent" or something similar, assuming that citizens cannot affirmatively assert their rights is a type of "save-people-from-themselves" paternalism that is misplaced both generally and in any type of Constitutional analysis. However, Professor Harris is correct in identifying a related, but separate, problem related to police-citizen encounters. Sometimes the police do not adhere to the citizen's assertion of their rights through refusing the officer's request to conduct a "consent-search." Obviously, the police must abide by a citizen's refusal to allow them to search if consent is the only applicable basis. Simply the fact that certain rogue officers may not follow these rules should not invalidate consent searches any more than the simple existence of coerced, non-voluntary confessions should invalidate *all* confessions. Interestingly, even when the police do affirmatively inform individuals of their right to refuse consent (similar to the manner in which the *Miranda* warnings provide individuals with notice of other rights) this is apparently not enough, and consent searches are somehow thought to be *per se* involuntary based on a numerical determination of how many consent versus how many refuse. If it all boils down to just "how people respond to authority" why would this same criticism not apply to countless other situations where individuals waive their constitutional rights? If the police do not act appropriately and honor a citizen's assertion of his or her right not to consent (given the overall circumstance), then this is an independent constitutional violation and should be dealt with accordingly. However, it should not act to invalidate all consent searches.

[53] *See* Dickerson v. United States, 530 U.S. 428, 443 (2000) ("*Miranda* has become embedded in routine police practice to the point where the warnings have become part of our national culture."). I have always found it personally perplexing that Chief Justice Rehnquist, historically a critic of *Miranda*, wrote the majority opinion in *Dickerson*, a 7-2 case in which Justices Scalia and Thomas (predictably) dissented. *Id.* at 430. For some insight into why the Chief Justice chose to author the opinion, and vote with the majority, see, Yale Kasimar, *Foreword: From* Miranda *to § 3501 to* Dickerson *to . . .*, 99 MICH. L. REV. 879, 889-90 (2001).

[54] "*Miranda* warnings" refers to warnings stemming from the United States Supreme Court's ruling in *Miranda v. Arizona*, 384 U.S. 436 (1966), *superseded by statute* 18 U.S.C. § 3501 (2000), and later re-affirmed in the Court's ruling in *Dickerson v. United States*, 530 U.S. 428 (2000). *See also* Donald A. Dripps, *Constitutional Theory for Criminal Procedure*: Dickerson, Miranda, *and the Continuing Quest for Broad but Shallow*, 43 WM. & MARY L. REV. 1 (2001); Yale Kasimar, *Can (Did) Congress "Overrule"* Miranda?, 85 CORNELL L. REV. 883, 930-36 (2000).

[55] *See generally* U.S. CONST. amend. V & VI. It is important to remember

al,[56] stupid decisions (especially in hindsight) on the part of individuals are not necessarily the by-product of government coercion.[57]

---

that there is a slightly different type of "waiver" that takes place with rights that are and are not enumerated in the *Miranda* warnings from those subject to custodial interrogation. *See* United States v. Barnett, 2004 WL 391830, at *4 (S.D. Ill. Feb. 27, 2004) ("However, the judge who considers the validity of a consent search of a home only needs to know if the rightful occupant of the search said yes when asked for consent and not whether that person was first advised of all her rights in detail as alluded to with the Fifth and Sixth Amendment rights above.") (citing Schneckloth v. Bustamonte, 412 U.S. 218 (1973)). *See* United States v. Drayton, 536 U.S. 194, 206 (2002) ("The Court has rejected in specific terms the suggestion that police officers must always inform citizens of their right to refuse when seeking permission to conduct a warrantless consent search."); *see also* Ohio v. Robinette, 519 U.S. 33, 39-40 (1996); Schneckloth v. Butsamonte, 412 U.S. 218, 227 (1973).

> Several commentators have supported a requirement that the police warn citizens of their right to refuse a request to search. They argue that the coercion citizens feel arises, at least in part, from the lack of knowledge of their right to refuse the request. One cannot refuse if one is not aware that refusal is an option. By requiring police to advise suspects that they can refuse to cooperate with the request to search, the argument goes, we remove the coercive aspect of the request and allow citizens to make a free and informed choice. The assumption is that if police are required to issue *Miranda*-type warnings in consent search cases, the compliance rate will necessarily decrease because, armed with the knowledge that refusal is an option, some people will choose to refuse. In fact, the majority in *Schneckloth* appears to have assumed that if warnings were required, virtually all citizens would refuse to consent to a search.
>
> That assumption turns out to be mistaken, at least in instances where it has been explicitly examined. A study of all Ohio highway stops conducted between 1995 and 1997 found no decrease in consent rates after police were required to advise motorists of their right to refuse to cooperate with a request for consent to search.

Nadler, *supra* note 52, at 204-05.

[56] *See, e.g.,* CTS Corp. v. Dynamics Corp. of Am., 481 U.S. 69, 96-97 (1987) (Scalia, J., concurring) ("But a law can be both economic folly and constitutional.").

[57] This statement is especially convincing in the context of probation where it is hard to say that accepting restrictive terms that may, at a later time, get one into further trouble, is a stupid or coerced decision when the alternative is prison. *See* United States v. Barnett, 415 F.3d 690, 692 (7th Cir. 2005) ("Here, given the alternative facing him of a prison sentence, Barnett gave up nothing."). Even in hindsight, the decision to avoid incarceration at all costs seems logical. How many inmates, even after the fact, would find it more appealing (or logical) to

In almost every case, the alternative to the relevant conditions of probation is incarceration.[58] Certain academics and practitioners have asserted that the agreement between a probationer, probation officials and court is the equivalent of a "probation contract" through which probationer effectively waives Fourth Amendment rights in exchange for the "consideration" of being placed on probation instead of going to prison.[59]

In this context, this argument can be referred to as the "California Approach" because of that State's longstanding acceptance of consent as a basis for the legality of broad-based probationary search conditions.[60]

---

accept incarceration instead of the privilege of probation.

[58] *See Barnett*, 415 F.3d at 692 (noting that claims made by offenders related to unreasonable searches must be viewed in light of fact that the greater deprivation of prison is the alternative to probation); United States v. Lifshitz, 369 F.3d 173, 179 (2d Cir. 2004) ("While upholding Fourth Amendment protections against unreasonable searches, we must therefore also remember that the alternative facing [probationer] in the absence of a computer monitoring probation condition might well be the more extreme deprivation of privacy wrought by imprisonment."). For comparative purposes, also see *Griffin*, 483 U.S. at 874 n.2 ("We have recently held that prison regulations allegedly infringing constitutional rights are themselves constitutional as long as they are 'reasonably related to legitimate penological interests.'" (quoting O'Lone v. Estate of Shabazz, 482 U.S. 342, 349 (1987))).

[59] In many cases, this consent argument stems from the fact that, if they do not want to choose probation, they can simply go to jail. Historically, this basic theory has been tagged the "Act of Grace" theory. *See, e.g.,* Note, *Judicial Review of Probation Conditions*, 67 COLUM. L. REV. 181, 188-91 (1967) (arguing that "Act of Grace" theory includes the notion that constitutional limitations do not exist if the defendant is granted the *privilege* of probation.). *But see* Brilliant, *supra* note 6, at 1367 n.61 (attempting to discredit "contract" theory of probation on the basis that an individual cannot consent to an illegal contract). It is completely unclear from the article what would make probation conditions that an offender agreed to in order to avoid the undoubtedly more restrictive option of incarceration *per se* "unconstitutional," "unreasonable," or illegal.

[60] *See, e.g.,* People v. Mason, 488 P.2d 630, 631 (Cal. 1971) (indicating California's longstanding approach going back over thirty years; case cited for historical relevance—negative history affects ruling's precedential value to date—however, bulk of related negative history is unpublished and noncitable), *overruled by* People v. Lent, 541 P.2d 545 (Cal. 1975). The California Supreme Court expressly acknowledges that an offender can refuse to consent to conditions of probation and simply go to jail. *Id.* at 632. ("If the defendant considers the

In *United States v. Knights*[61] (discussed in detail in Part V.), the United States Supreme Court acknowledged the consent argument but did not reach the merits of it. "We need not decide whether Knights' acceptance of the search condition constituted consent in the *Schneckloth* sense of a complete waiver of his Fourth Amendment rights, however, because we conclude that the search of Knights was reasonable under our general Fourth Amendment approach . . . ."[62]

While the United States Supreme Court has not addressed this question directly, a recent Seventh Circuit opinion, *United States v. Barnett,*[63] specifically addressed the question that *Knights* left open: "whether the waiver alone could justify the search."[64]

After being convicted in an Illinois state court of aggravated fleeing from police, criminal damage to state property, and damage to property, Barnett was "sentenced to a year of 'Intensive Probation Supervision' [IPS] in lieu of prison" as part of a plea bargain.[65]

---

conditions of probation more harsh than the sentence the court would otherwise impose, he has the right to refuse probation and undergo the sentence."); *see also* People v. Bravo, 738 P.2d 336, 339-40 (Cal. 1987). The court, in *Bravo*, held that defendant's waiver of Fourth Amendment rights should be viewed in light of an objective, not subjective, test. *Id.* Further, the court held that such searches cannot be for reasons of harassment or searches for arbitrary or capricious reasons. *Id.* at 342-43. "We do not suggest that searches of probationers may be conducted for reasons unrelated to the rehabilitative and reformative purposes of probation or other legitimate law enforcement purposes. A waiver of Fourth Amendment rights as a condition of probation does not permit searches for arbitrary or capricious reasons." *Id.* (citations omitted); *see also* People v. Reyes, 968 P.2d 445, 450 (Cal. 1998); *In re* Tyrell J., 876 P.2d 519, 521 (Cal. 1994).

[61] 534 U.S. 112 (2001).

[62] *Id.* at 118.

[63] 415 F.3d 690 (7th Cir. 2005). The decision is authored by Circuit Judge Posner, one of this Nation's most noted jurists. *Id.* at 691.

[64] *Id.* The court also refers to this question as one of "the validity of a blanket waiver of Fourth Amendment rights as a condition of probation." *Id.*; *see also* United States v. Lifshitz, 369 F.3d 173, 182 (2d Cir. 2004) (relating to question left by Court in *Knights*); United States v. Brown, 346 F.3d 808, 812 (8th Cir. 2003) (same); United States v. Vaval, 404 F.3d 144, 152-53 (2d Cir. 2005) ("[B]ecause plea bargains require defendants to waive fundamental constitutional rights, prosecutors are held to meticulous standards of performance." (citing United States v. Lawlor, 168 F.3d 633, 637 (2d Cir. 1999))).

[65] *Barnett*, 415 F.3d at 691. "[Barnett's] lawyer acknowledges having bargained

One of the conditions of IPS required Barnett to "[S]ubmit to searches of [his] person, residence, papers, automobile and/or effects at any time such requests are made by the Probation Officer, and consent to the use of anything seized as evidence in Court proceedings."[66]

During his period of probation, Barnett's home was searched by a probation officer.[67] During this search, a gun was discovered and Barnett was charged with being a felon in possession of a firearm.[68]

---

for this disposition, which Barnett preferred to a prison sentence." *Id.* These charges are the underlying charges for which Barnett was on a term of probation. The instant case, and the Seventh Circuit ruling, stem from an attempt to suppress evidence revealed in a search related to a charge of being a felon in possession of a gun. *Id.*

[66] *Id.* at 691-92. Obviously, where consent is the basis for Fourth Amendment waiver, the express language of the probation condition would control the breadth and scope of the waiver. *Id.* at 692.

[67] The probation officer was accompanied by two sheriff's deputies. United States v. Barnett, No. 03-CR-30170, 2004 WL 391830, at *2 (S.D. Ill. Feb. 27, 2004) (footnote omitted).

[68] *Id.* As indicated *supra* note 40 and accompanying text, where consent is at issue, the surrounding facts and circumstances, as well as the express condition previously agreed to, must be considered. The facts of the warrantless search at issue in *Barnett* are as follows:

> On April 15, 2003, George Chester, the supervisor of the Intensive Probation Supervision Unit of the Probation Department, sought authority from the St. Clair County State's Attorney's Office to conduct a warrantless search of Barnett's residence. Chester felt that Barnett's actions in his office that day established reasonable suspicion of illegal contraband or activity. His [sic] based his belief on Barnett's reaction to an arrest effected that day for Barnett's failure to appear in court on some undisclosed matter. Chester testified that Barnett "overreacted" to that arrest, for the purported reason that Barnett had a woman in his car whom he did not want his wife to discover. Following the encounter with Barnett, Chester looked more fully into Barnett's criminal background and found five felony convictions and numerous domestic battery issues. Based on these findings, Chester determined that there was reasonable suspicion that illegal contraband or activity was to be found at Barnett's house. On the strength of that hunch, Chester received permission to search Barnett's home from the State's Attorney's Office.
>
> Consequently, in the evening hours of the same day, Probation Officer Rodney Skinner was directed to conduct a search of Barnett's residence. Officer Skinner, accompanied by two sheriff's deputies for assistance, went to Barnett's home.

Judge Posner's opinion in *Barnett* is dually-rooted in two primary themes: (1) Constitutional rights can be waived;[69] and (2) "[p]lea bargains are a form of contract."[70]

### *i. Waiver*

The issue of whether Constitutional rights can be waived is settled law;[71] however, the specific question addressed in *Barnett* is "whether the waiver alone could justify the search."[72] While the semantic error is likely harmless overall, the Seventh Circuit's "sufficiency" inquiry into the waiver doctrine appears misplaced. The question is actually: (1) does the Fourth Amendment apply;[73] (2) if so, does consent to a

---

*Id.* at *2 (footnote omitted). This "search" falls into several grey areas for the purposes of the factual scenarios set forth in Part I(ii), *supra*. It appears that this "search" has elements of FP1—depending on the level of suspicion that was present at the time the search was initiated. Although Supervisor Chester acted on a "hunch" that may or may not have risen to the level of "reasonable suspicion," the government itself did not claim that "reasonable suspicion" existed at the time instructions were issued to probation officer. Skinner. *See Barnett*, 2004 WL 391830, at *2. "Secondly, while not suggesting the reasonable suspicion existed when the instructions were issued by Supervisor Chester to Officer Skinner for the search . . . ." *Id.* Here, the evidence was used to prosecute Barnett for a new crime (possession of firearm by felon) and not simply to administratively revoke his probation. *Id.* Also, although it appears that the sheriff's deputies accompanied P.O. Skinner to execute the search, it appears that this action was taken unilaterally by probation authorities (with the permission of the State's Attorney's Office). *Id.* ("accompanied by two Sheriff's Department deputies *for assistance* . . . .") (emphasis added).

[69] *See Barnett*, 415 F.3d at 691. "Constitutional rights like other rights can be waived, provided that the waiver is knowing and intelligent, as it was here." *Id.*

[70] *Id.* at 692. "Plea bargains are a form of contract, and like other contracts are presumed to make both parties better off and do no harm to third parties, and so they are enforceable and enforced. Here, given the alternative facing him of a prison sentence, Barnett gave up nothing." *Id.* (citations omitted).

[71] "Waiver of [a specific constitutional right], as of constitutional rights in the criminal process generally, must be a 'knowing, intelligent ac[t] done with sufficient awareness of the relevant circumstances.'" Halbert v. Michigan, 125 S. Ct. 2582, 2594 (2005) (citations omitted); Johnson v. Zerbst, 304 U.S. 458, 464 (1938). The Court does not favor "waiver" of fundamental rights. *See* Carnley v. Cochran, 369 U.S. 506 (1962); Ohio Bell Tel. Co. v. Public Utils. Comm'n, 301 U.S. 292, 307 (1937); Aetna Ins. Co. v. Kennedy, 301 U.S. 389, 393 (1937) (courts should "indulge every reasonable presumption against waiver.").

[72] *Barnett*, 415 F.3d at 691.

[73] The Fourth Amendment only applies when a search is conducted that in-

probation condition allowing a certain type of search amount to "waiver;" and, (3) if so, did the individual with Fourth Amendment standing waive his/her right(s) under the Amendment by consenting? The question is whether there was, in fact, a waiver, not whether there was sufficiency of such a waiver assuming it exists.[74]

### *ii. Contract-law analogy/analysis*

Plea bargains are a crucial part of the American criminal justice system.[75] The Seventh Circuit held that the plea bargain can be viewed, and reviewed, as "a form of contract."[76] The use of contract law for the basis of analysis in reviewing plea bargains has also been used when the government is accused of "breach."[77]

---

fringes upon an individual's reasonable expectation of privacy. United States v. Reyes, 283 F.3d 446, 471 (2002). For an individual's expectation of privacy to be legitimate, she must exhibit "an actual (subjective) expectation of privacy and the expectation must be one that society is prepared to recognize as reasonable." *Id.* at 457 (internal quotations omitted).

[74] While after-the-fact "sufficiency" of an established waiver is irrelevant in my view, as the constitutional inquiry is over, one still must determine whether the waiver ever came into existence in the first place, i.e., whether it is a valid waiver. Constitutional rights can be waived. *See generally*, Schneckloth v. Bustamonte, 412 U.S. 218 (1973).

[75] *See* Bordenkircher v. Hayes, 434 U.S. 357, 361-62 (1978) ("We have recently had occasion to observe: '[W]hatever might be the situation in an ideal world, the fact is that the guilty plea and the often concomitant plea bargain are important components of this country's criminal justice system. Properly administered, they can benefit all concerned.'") (citations omitted). "Plea bargaining flows from 'the mutuality of advantage' to defendants and prosecutors, each with his own reasons for wanting to avoid trial." *Bordenkircher*, 434 U.S. at 363 (quoting Brady v. United States, 397 U.S. 742, 752 (1970)).

[76] United States v. Barnett, 415 F.3d 690, 692 (7th Cir. 2005). ("Plea bargains are a form of contract . . . ."). Other circuits have similarly applied the contract analysis when reviewing plea bargains. *See* United States v. Vaval, 404 F.3d 144, 152 (2d Cir. 2005) (quoting United States v. Riera, 298 F.3d 128, 133 (2d Cir. 2002)) ("We review interpretations of plea agreements de novo and in accordance with principles of contract law.").

[77] *See, e.g.*, *Vaval*, 404 F.3d at 152-53.

> Further, we construe plea agreements strictly against the government and do not "hesitate to scrutinize the government's conduct to ensure that it comports with the highest standard of fairness." *United States v.*

The Seventh Circuit correctly identifies the "bargain" that takes place in a plea bargain, stating, "[o]ften a big part of the value of a right is what one can get in exchange for giving it up."[78] The court also dismisses what is basically a general warrant claim[79] based on theories of contract law:

> [C]ontracts (. . . remember that the plea bargain, containing the consent to searches, is to be interpreted as a contract) contain implicit as well as explicit terms. Especially implicit terms necessary to head off absurdities.[80]

In *Barnett*, the Seventh Circuit, finding that a plea bargain which amounts to a waiver of Fourth Amendment rights should be reviewed under the tenets of contract law, firmly answered the question left open by the Supreme Court in *Knights*, finding that "waiver [alone] could justify the search."[81] Obviously,

---

> *Lawlor*, 168 F.3d 633, 637 (2d Cir. 1999). "To determine whether a plea agreement has been breached, a court must look to what the parties reasonably understood to be the terms of the agreement." *Id.* at 636 (internal quotation marks and citation omitted). Moreover, because plea bargains require defendants to waive fundamental constitutional rights, prosecutors are held to meticulous standards of performance. *Id.*

*Id.*

[78] *Barnett*, 415 F.3d at 692.

[79] *See, e.g.,* Illinois v. Krull, 480 U.S. 340, 362 (1987) (O'Connor, J., dissenting) ("This Court has repeatedly noted that reaction against the ancient Act of Parliament authorizing indiscriminate general searches by writ of assistance, 7 & 8 Wm. III, c. 22, § 6 (1696), was the moving force behind the Fourth Amendment.").

[80] *Barnett*, 415 F.3d at 692. (citations omitted). "[A] contract will not be interpreted literally if doing so would produce absurd results, in the sense of results that the parties, presumed to be rational persons pursuing rational ends, are very unlikely have agreed to seek." Beanstalk Group, Inc. v. AM Gen. Corp., 283 F.3d 856, 860 (7th Cir. 2002). Other contract law limitations (duress, mistake, unconscionability, and public policy concerns) could come into play in a contract-based analysis. *See* Blank, *supra* note 43 and accompanying text.

[81] *See supra* Part III(i) "waiver" for explanation of why I do not believe the "alone" here is relevant. If the right is validly waived, then the protections of the Fourth Amendment do not apply for purposes of analysis, and the defendant has no standing to assert the waived rights. I reject what I believe is a type of "sufficiency of waiver" inquiry. It does appear that certain types of "waiver of rights" doctrine might fail under contract law analysis. *See, e.g.,* Blank, *supra* note 43, at 2074.

if waiver under contract law is to control, the express terms of the condition become *extremely* important.[82] With regards to the two factual scenarios set forth in Part I(ii), *supra*, what type of government agency can search, what they can look for, and what they can do with what they discover with regards to

---

> Thus, the contract principles of adhesion, duress, mistake, unconscionability, and public policy all suggest that, even if the practice of plea bargaining as a whole can pass constitutional muster under contract analysis, waivers of the right to disclosure of *Brady* material cannot. Accordingly, under a contract-based approach, a defendant may not waive his *Brady* rights as part of a plea bargain.

*Id.*

[82] For an example of the United States Supreme Court returning to the express language of the probation condition for guidance, see the Court's unanimous opinion in *United States v. Knights*, 534 U.S. 112, 116 (2001) ("Certainly nothing in the condition of probation suggests that it was confined to searches bearing upon probationary status and nothing more. The search condition provides that Knights will submit to a search "by any probation officer or law enforcement officer" and does not mention anything about purpose."); *see also* United States v. Stanfield, 360 F.3d 1346, 1353-54 (D.C. Cir. 2004) (example of vague condition hindering analysis by reviewing court).

> We are reluctant to address the validity of the internet restriction in the absence of a clearer understanding of its scope; we need more solid footing before deciding where we stand. The evolutionary process the internet restriction has undergone in this case—involving challenges by the defendant, redefinition by the district court without providing notice to or hearing argument from the defendant, and sporadic concessions by the government—has culminated in a lack of clarity about what exactly is before us. That is problematic enough as a general matter; neither the defendant nor the probation office and district court should have to consult the judgment, the briefs before this court, and the transcript of oral argument to determine the scope of the condition. Subsection (f) of 18 U.S.C. § 3583 specifies that:
>
>> The court shall direct that the probation officer provide the defendant with a written statement that sets forth all the conditions to which the term of supervised release is subject, and that is sufficiently clear and specific to serve as a guide for the defendant's conduct and for such supervision as is required.
>
> *See also* United States v. Simmons, 343 F.3d 72, 81 (2d Cir. 2003) ("Due process requires that the conditions of supervised release be sufficiently clear to give the person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may act accordingly") (internal quotation marks and citations omitted).

*Stanfield,* 360 F.3d at 1353-54.

a given probationer will depend on the terms of the contract the offender entered into and the scope of search anticipated in that contract. Returning briefly to Judge Posner's opinion in *Barnett*, "contracts are presumed to make both parties better off and do no harm to third parties,[83] and so they are enforceable and enforced."[84] The person can go to prison, if he or she so choose. It is a bad option, and some will say that this smacks of being a contract of adhesion.[85] Nonsense, it is a bad option because the person (for some reason, believing it to be to their advantage) has just pled guilty to a charge involving Internet-related child pornography.[86] Are we, as a society, really concerned with providing good options for this individual? The fact that the option (or contract) of probation exists at all amounts to a *privilege* and not a right.[87] I believe that the Court, at some point, will answer the question it left open in 2001 in accordance with the Seventh Circuit's opinion in *Barnett*.[88] However, in the meantime, or if I am simply wrong, analysis under the Fourth Amendment becomes necessary.

---

[83] There is a fascinating collateral issue to this analysis that is outside the scope of this article. Given that contracts are generally enforceable when they "do no harm to third parties," what if the victim (or victim's family) in a case do not agree with the plea bargain and believe that the defendant is getting off too "light"? Should the victim's detriment, as a third party under contract law, invalidate the plea agreement (contract) and render it void?

[84] *Barnett*, 415 F.3d at 692. The Seventh Circuit details this tenet within the facts of the instant case.

> Barnett didn't want to go to prison. He preferred to sacrifice the limited privacy to which he would have been entitled had he been on ordinary as distinct from intensive probation (as we'll see), just as convicted defendants prefer home confinement to confinement in a jail or prison even if the home confinement involves monitoring the defendant's activities inside the home and thus invades his privacy. And since imprisonment is a *greater* invasion of personal privacy than being exposed to searches of one's home on demand, the bargain that Barnett struck was not only advantageous to him but actually more protective of Fourth Amendment values than the alternative of prison would have been. It was also advantageous to the government, which wouldn't have agreed to it otherwise.

*Id.* at 691-92.

[85] *See, e.g.,* United States v. Messanatto, 513 U.S. 196, 216 (1995) (Souter, J., dissenting) ("As the Government conceded during oral argument, defendants are generally in no position to challenge demands for these waivers, and the use of waiver provisions as contracts of adhesion has become accepted practice."). They are in a position—they can assert their right to trial to be found not guilty if they are maintaining their innocence. If they are conceding guilt, *yes, there is no good choice*; the only question is which is the best option within a host of "bad" choices. This does not make their exercise of bargaining for the best possible option a contract of adhesion. *See, e.g.,* Robert E. Scott & William J. Stuntz, *Plea Bargaining as Contract*, 101 YALE L.J. 1909, 1922 (1992) (noting contrasting characteristics between plea bargains and contracts of adhesion).

[86] The person may also be found guilty and the only comparison is probation

## PART IV. FOURTH AMENDMENT FRAMEWORK--GENERALLY

Under the Fourth Amendment, the "ultimate measure of the constitutionality of a governmental search is 'reasonableness.'"[89] To determine whether a search meets the reasonableness standard, "'it is judged by 'balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests.'"[90] Generally, for a search conducted by law enforcement to be "reasonable" under the Fourth Amendment, a warrant is required.[91] The Fourth Amendment only applies when a search is conducted that infringes upon an individual's reasonable expectation of privacy.[92] For an individual's expectation of privacy to be legitimate, she must exhibit "an actual (subjective) expectation of privacy and the expectation [must] be one that society is prepared to recognize as 'reasonable.'"[93]

---

(regardless of how restrictive) and prison.

[87] *See, e.g.,* Escoe v. Zerbst, 295 U.S. 490, 492-93 (1935) ("Probation or suspension of sentence comes as an act of grace to one convicted of a crime, and may be coupled with such conditions . . . .") (citing Burns v. United States, 287 U.S. 216 (1932)).

[88] *See supra* notes 62-64 and accompanying text. The Court expressly reserved two major questions in *Knights:* (1) whether probation "so diminished or completely eliminated [offenders'] reasonable expectation of privacy"; or (2) whether accepting the terms of probation "constituted consent." United States v. Knights, 534 U.S. 114, 120 n.6 (2001).

[89] Vernonia Sch. Dist. v. Acton, 515 U.S. 646, 652 (1995).

[90] *Id.* at 652-53 (quoting Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 619 (1989)).

[91] *Id.*

[92] The modern Fourth Amendment privacy definition was set forth in Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[93] *Id.*; *see also* United States v. Reyes, 283 F.3d 446, 457 (2d Cir. 2002);

In 2001, in a unanimous opinion, the Court basically commanded the broad strokes of the framework I detail in parts V & VI. The two primary Supreme Court cases are expressly distinguished from one another and leave open the possibility that either a general standard of reasonableness or the Fourth Amendment exception under the special needs doctrine will be utilized and, therefore, applicable:

> In Knights' view, apparently shared by the Court of Appeals, a warrantless search of a probationer satisfies the Fourth Amendment only if it is just like the search at issue in *Griffin, i.e.,* a "special needs" search conducted by a probation officer monitoring whether the probationer is complying with probation restrictions. This dubious logic—that an opinion upholding the constitutionality of a particular search implicitly holds unconstitutional any search that is not like it—runs contrary to *Griffin's* express statement that its "special needs" holding made it "unnecessary to consider whether" warrantless searches of probationers were otherwise reasonable within the meaning of the Fourth Amendment.[94]

In other words, because the Court based its ruling in *Knights* on reasonableness, it did not consider the alternative "special needs" analysis under *Griffin*; because the *Griffin* Court found the special needs analysis adequate, it found it "unnecessary" to consider warrantless probationary searches under a standard of general reasonableness.[95]

---

WEAVER ET AL, PRINCIPLES OF CRIMINAL PROCEDURE 82-88 (2004). It seems settled that probationers have, at most, a "significantly diminished . . . reasonable expectation of privacy." *Knights*, 534 U.S. at 119-20. "We do not decide whether the probation condition so diminished, or completely eliminated, [probationer's] reasonable expectation of privacy . . . ." *Id.* at 120 n.6. Similar to a situation where the United States Supreme Court holds the issue of waiver, considered above, if the Court would hold that probationer's simply have no reasonable expectation of privacy in relation to such searches, the analysis would be effectively over.

[94] *Knights*, 534 U.S. at 117-18 (citations omitted).

[95] *Id.*

## PART V. "TRACK I" REASONABLENESS

The landmark, and most relevant, case for "Track I" analysis in the context of warrantless probationary searches is *United States v. Knights*.[96] In *Knights*, a unanimous United States Supreme Court held that the probationary search in question was supported by "reasonable suspicion" and was therefore "reasonable" under general Fourth Amendment analysis.[97]

### *i. Facts-United States v. Knights*

Mark James Knights was on probation for a drug offense.[98] The terms of probation included the condition, "That Knights would '[s]ubmit his . . . person, property, place of residence, vehicle, personal effects, to search at anytime, with or without a search warrant, warrant of arrest or reasonable cause by any probation officer or law enforcement officer.'"[99] Between 1996 and 1998, the facilities of the Pacific Gas and Electric Company (PG&E) in Napa County, California were vandalized over thirty times.[100] Because the vandalism began after Knights' electric service was discontinued and the incidents coincided with his court appearances over his theft of power from PG&E, suspicion focused on Knights.[101] On June 3, 1998, the local sheriff's department set up surveillance on

---

[96] 534 U.S. 112 (2001).

[97] *Knights*, 534 U.S. at 122 ("Because our holding rests on ordinary Fourth Amendment analysis that considers all the circumstances of a search, . . . ."); *see also id.* at 118 ("[W]e conclude that the search of Knights was reasonable under our general Fourth Amendment approach of 'examining the totality of the circumstances,' with the probation search condition being a salient circumstance.") (citation omitted).

[98] *Knights*, 534 U.S. at 114.

[99] *Id.* This is a broad probation condition in this context as it allows not only the warrantless search, but also that the search can be conducted by either probation or law enforcement officers generally. *Id.* "Knights signed the probation order, which stated immediately above his signature that 'I HAVE RECEIVED A COPY, READ AND UNDERSTAND THE ABOVE TERMS AND CONDITIONS OF PROBATION AND AGREE TO ABIDE BY SAME.' App. 49.").

[100] United States v. Knights, 219 F.3d 1138, 1140 (9th Cir. 2000), *rev'd*, 534 U.S. 112 (2001).

[101] *Id.*

Knights' apartment.[102] Steven Simoneau, a friend of Knights, was seen leaving the apartment carrying what appeared to be three pipe bombs.[103] Simoneau was next seen crossing the street to a river, where he deposited the suspected pipe bombs.[104] A detective followed Simoneau's truck until it pulled into a driveway.[105] After Simoneau exited and walked away from the truck, the detective was able to look at the truck unobserved.[106] In and around the truck, the detective found a Molotov cocktail, explosive materials, a gasoline can, and two brass padlocks.[107] The sheriff's department seized the truck, impounded it and searched it pursuant to a warrant at a later time.[108] Knowing the connection between Simoneau and Knights, the fact that he had come directly from Knights' apartment and the fact that he was a probationer whose probation included a general law-enforcement search term, Detective Hancock decided to conduct a warrantless search of Knights' apartment.[109] The search "turned up detonation cord, ammunition, unidentified liquid chemicals, instruction manuals on chemistry and electrical circuitry, bolt cutters, telephone pole-climbing spurs, drug paraphernalia, photographs and blueprints stolen from the burglarized building, and a brass padlock stamped PG&E."[110] Knights was indicted in federal court for "conspiracy to commit arson, for possession of an unregistered destructive device, and for being a felon in possession of ammunition."[111]

---

[102] *Id.*

[103] *Id.*

[104] *Id.*

[105] *Id.*

[106] *Id.*

[107] *Id.* These padlocks fit the description of padlocks removed from a recently-vandalized electric transformer. *Id.*

[108] *Id.* Although a warrant was secured in this instance, if the vehicle was impounded legitimately, the "inventory" exception could have come into play. *See, e.g.*, South Dakota v. Opperman, 428 U.S. 364 (1976).

[109] *Knights*, 219 F.3d at 1140-41. Prior to conducting the search, Detective Hancock received permission from his supervisor. *Id.* "Detective Hancock was aware of the search condition in Knights' probation order and thus believed that a warrant was not necessary." *Knights*, 534 U.S. at 115. "Hancock had seen a copy of the probation order when he was checking Knights' file in the Sheriff's Department office." *Id.* at n.1. In this context, I am acknowledging, but not going to address in detail, whether the "good-faith" exception would apply to this type of situation. If the officer believes in "good-faith" that he is acting pursuant to a statute, in this instance one that would allow a warrantless search, and that statute is later found unconstitutional, a "good faith" exception can apply for statutes similar to the one found in the *Leon*-exception for warrants. *See* Illinois v. Krull, 480 U.S. 340 (1987). Given that explosives were involved, and the large-scale damage this type of vandalism can create, there is a possibility that exigency could be the basis of a warrantless search of Knights' apartment. *See* McDonald v. United States, 335 U.S. 451, 454 (1948); People v. Sirhan, 497 P.2d 1121,

### *ii. The "Reasonableness" Approach*

Any approach based on how reasonable something is (or is not) in a particular context, whether it is to review the actions or inactions of a "reasonable person" or to review whether the government has conducted a "reasonable" warrantless search is inherently subjective.[112]

In *Knights*, the Court expressly declined to apply any type of "special needs" analysis (set forth in detail in Part VI) and instead applied a general balancing of interests to determine whether the search passed constitutional muster.[113]

---

1138-39 (1972), *overruled by* Hawkins v. Superior Court, 586 P.2d 916 (Cal. 1978).

[110] *Knights*, 219 F.3d at 1141.

[111] *Id. See* 18 U.S.C. §§ 371, 922(g); 26 U.S.C. § 5861(g). The district court suppressed the evidence seized from Knights' apartment, holding that the "probation search was really a subterfuge for an investigative search." *Knights*, 219 F.3d at 1141. The Ninth Circuit upheld the district court's ruling. *Id.* at 1145. *Certiorari* was granted on May 14, 2001.

[112] *See* Abner S. Greene, *Is There a First Amendment Defense for* Bush v. Gore?, 80 NOTRE DAME L. REV. 1643, 1677 (2005) ("If the terms of a law are sufficiently clear to guide a reasonable person in her conduct, then the law will overdeter, stopping people from engaging in conduct because they are unsure of the law's sweep.").

[113] *Knights*, 534 U.S. at 117-18.

> In Knights' view, apparently shared by the Court of Appeals, a warrantless search of a probationer satisfies the Fourth Amendment only if it is just like the search at issue in *Griffin*—i.e., a "special needs" search conducted by a probation officer monitoring whether the probationer is complying with probation restrictions. This dubious logic—that an opinion upholding the constitutionality of a particular search implicitly holds unconstitutional any search that is not like it—runs contrary to *Griffin's* express statement that its "special needs" holding made it "unnecessary

Similar to the importance of the de facto review of the express probation condition if a contract analysis is to be applied (Part IV(ii)) a reasonableness analysis must make a de facto review of all of the relevant facts and circumstances surrounding the search at issue. For this reason, even given that it is a recent, unanimous, opinion of the Supreme Court, *Knights* can only reveal how the Court rules on a particular search.[114] Our analysis is based, therefore, on analogizing a future, hypothetical search that might be challenged under the *Knights* ruling and the framework the Court applied.

The Court recognizes reasonableness as "[t]he touchstone of the Fourth Amendment" and states that the balance to be considered is "on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[115]

In the context of probation, the Court clearly identified the "balance" it would utilize:

> Knights' status as a probationer subject to a search condition informs both sides of that balance. "Probation, like incarceration, is 'a form of criminal sanction imposed by a court upon an offender after verdict, finding, or plea of guilty.'" Probation is "one point . . . on a continuum of possible punishments ranging from solitary confinement in a maximum-security facility to a few hours of mandatory community service." Inherent in the very nature of probation is that probationers "do not enjoy 'the absolute liberty to which every citizen is entitled.'"[116]

---

> to consider whether" warrantless searches of probationers were otherwise reasonable within the meaning of the Fourth Amendment.

*Id.* (citations and footnotes omitted). For an exhaustive review of the concept of reasonableness, see generally, Thomas K. Clancy, *The Fourth Amendment's Concept of Reasonableness*, 2004 UTAH L. REV. 977 (2004).

[114] *Knights*, 534 U.S. at 121 ("We hold that the balance of these considerations requires no more than reasonable suspicion to conduct a search of *this probationer's* house.") (emphasis added).

[115] *Id.* at 118 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

[116] *Id.* at 119 (citations omitted).

After determining that the search condition was relevant within the larger framework of Knights' probation, properly limiting his rights in relation to his status as a probationer, the Court concluded that the search provision "would further the two primary goals of probation—rehabilitation and protecting society from future criminal violations."[117]

Although the Court does not reach the full merits of the consent argument,[118] it ruled that, due to the fact that "Knights was unambiguously informed of [the search condition]," the information acted to significantly diminish "his expectation of privacy."[119] After determining that Knights did have some reasonable expectation of privacy with regards to the search of his home,[120] the Court assessed the governmental interest in the balancing test.[121] Finding that probationers

---

[117] *Id.*

[118] *See supra* note 62 and accompanying text.

[119] *Knights*, 534 U.S. at 119-20.

[120] *Id.* at 118-19. The Court did not make this determination in the positive. Similar to its decision not to rule decisively on the consent/waiver aspect of the case, *see supra* note 62 and accompanying text, the Court similarly does not rule on whether the probation condition completely eliminated Knights' reasonable expectation of privacy in the context of the Fourth Amendment. *Knights*, 534 U.S. at 120 n.6.

> We do not decide whether the probation condition so diminished, or completely eliminated, Knights' reasonable expectation of privacy (or constituted consent, *see supra*, at 118) that a search by a law enforcement officer without any individualized suspicion would have satisfied the reasonableness requirement of the Fourth Amendment. The terms of the probation condition permit such a search, but we need not address the constitutionality of a suspicionless search because the search in this case was supported by reasonable suspicion.

*Id.*

[121] *Id.* at 120-21. The Court provided additional details about the "balance" at issue:

> The State has a dual concern with a probationer. On the one hand is the hope that he will successfully complete probation and be integrated back into the community. On the other is the concern, quite justified, that he will be more likely to engage in criminal conduct than an ordinary member of the community. The view of the Court of Appeals in this case would require the State to shut its eyes to the latter concern and concentrate only on the former. But we hold that the Fourth Amendment does not put the State to such a choice. Its interest in ap-

are more likely to violate the law, generally, the Court held that "the balance of these considerations requires no more than reasonable suspicion to conduct a search of this probationer's house."[122]

This reasonableness inquiry is, by nature, an ad hoc analysis. For general comparison purposes, it appears clear, after *Knights*, that the search in FP1[123] would be reasonable so long as the government was acting with "reasonable suspicion."[124] FP2 would also likely be deemed reasonable, if chal-

---

> prehending violators of the criminal law, thereby protecting potential victims of criminal enterprise, may therefore justifiably focus on probationers in a way that it does not on the ordinary citizen.

*Id.*

[122] *Id.* at 121; *see supra* note 109 and accompanying text. The Court was cognizant that "probable cause" was the ordinary level of probability necessary to satisfy the Fourth Amendment, but "a lesser degree satisfies the Constitution when the balance of governmental and private interests makes such a standard reasonable." *Knights*, 534 U.S. at 121 (citing Terry v. Ohio, 392 U.S. 1 (1968); United States v. Brignon-Ponce, 422 U.S. 873 (1975)). "In *Knights*, however, the Court refrained from upholding generally the search condition that had been imposed—which, on its face, would have permitted suspicionless searches—and decided only that the particular search at issue met the requirements of the Fourth Amendment . . . ." United States v. Lifshitz, 369 F.3d 173, 180 (2d Cir. 2004).

[123] *See supra* Part I(ii)(1).

[124] As the exclusionary rule does not apply to probation revocation hearings, FP2 is also the least likely to be contested given that any evidence gathered will be suppressed and inadmissible in a judicial hearing and there is no remedy which would allow it to be directly appealed for purposes of revocation generally. In *United States v. Yuknavich*, 419 F.3d 1302, 1309-10 (11th Cir. 2005), the Eleventh Circuit applied the *Knights* balancing test where there was not a specific condition related to warrantless searches.

> The only major difference between the case before us and *Knights* is that Knights' probation agreement contained a provision explicitly requiring him to submit to warrantless searches, whereas no such provision is present here. We must consider whether, in this case, the lack of search condition upsets the *Knights* balancing test so as to require more than reasonable suspicion to justify a search of Yuknavich's computer. *Cf. United States v. Brown*, 346 F.3d 808, 812 (8th Cir. 2003) (considering "whether, given the scope of Brown's probationary condition, the presence of the additional personnel sway[ed] the [*Knights*] balancing test").
>
> . . . .
>
> In sum, assuming the lack of a search condition heightened Yuknavich's expectation of privacy, it did not sway the *Knights* balancing test such that the probation officers needed more than reasonable suspi-

lenged at all, because the search and/or monitoring is conducted pursuant to a valid probation condition and any evidence gathered is only intended for use at an administrative probation revocation hearing.

## PART VI. TRACK II SPECIAL NEEDS

### *i. The "Special Needs" Approach*

Although the predominant rule requires a judicial warrant based on probable cause,[125] the Court has recognized exceptions to this rule "when '*special needs*, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.'"[126] "Special needs" have been recognized in a variety of contexts including "[t]he Government's interest in . . . its supervision of probationers."[127]

Tracey Maclin has stated, correctly in my view, that "[w]hile the Court has issued several rulings under its 'special needs' analysis, these cases do not form a coherent doctrine."[128]

---

cion to conduct a search of Yuknavich's computer.

*Id.* at 1309, 1311.

[125] *See, e.g.,* Payton v. New York, 445 U.S. 573, 588 n.26 (1980).

[126] Skinner v. Ry Labor Executives' Ass'n, 489 U.S. 602, 619 (1989) (quoting Griffin v. Wisconsin, 483 U.S. 868, 873 (1987) (citation omitted) (emphasis added).

[127] *Id.* at 620; *see also* Bd. of Educ. of Indep. Sch. Dist. No. 92 v. Earls, 536 U.S. 822 (2002) (applying Fourth Amendment "special needs" doctrine to school drug testing of students involved in extracurricular activities); Chandler v. Miller, 520 U.S. 305 (1997) (applying Fourth Amendment "special needs" doctrine to mandatory drug testing for political candidates); Vernonia Sch. Dist. v. Acton, 515 U.S. 646 (1995) (applying Fourth Amendment "special needs" doctrine to school drug testing of student-athletes); New Jersey v. T.L.O., 469 U.S. 325 (1985) (applying Fourth Amendment "special needs" doctrine to in-school searches of students conducted by faculty).

[128] Tracey Maclin, *Is Obtaining an Arrestee's DNA a Valid Special Needs Search Under the Fourth Amendment? What Should (and Will) the Supreme Court Do?*, 33 J.L. MED. & ETHICS 102, 107 (2005); *see also* Thomas K. Clancy, *The Role of Individualized Suspicion in Assessing the Reasonableness of Searches and Seizures*, 25 U. MEM. L. REV. 483, 597 (1994) (indicating some confusion in the name and actual application of the doctrine).

> The Supreme Court has also not required individualized suspicion when a "special need" of the government is present. The term "special

In the context of warrantless searches, the "special needs" exception gained a head of steam between 1989 and 1995 and seemed poised to emerge as the rule instead of the exception. The Court appeared to have abandoned the original constructs (1) that "'*special needs*' be beyond the normal need for law enforcement;" and (2) the type of search at issue "make the warrant and probable-cause requirement impracticable."[129]

However, in 1995, the Court, in *Chandler v. Miller*,[130] appeared to want to "cabin the earlier decisions upholding suspicionless searches as belonging to a 'closely guarded category' of cases 'involving limited circumstances.'"[131] If *Chandler* slowed the "special needs" train, the Court, in *City of Indianapolis v. Edmond*[132] and *Ferguson v. City of Charleston,*[133] seemed to want to return the "special needs" doctrine to its roots.[134] Viewed collectively, *Edmond* and

---

> need," however, is misleading. The Court is not referring to any "need" in the sense of necessity; rather, it speaks of a special *interest*. Also, although the initial cases adopting the concept involved governmental regulatory interests unrelated to criminal penalties, the Court has now excised from the definition of a special need the requirement that the interest must be unrelated to criminal law enforcement. What is considered a special need has evolved to include some very mundane criminal law enforcement concerns.

*Id.* (emphasis added).

[129] *See supra* note 126 and accompanying text.

[130] 520 U.S. 305 (1997) (striking law that required drug testing for all candidates seeking certain state offices).

[131] Sundby, *supra* note 7, at 516. "The *Chandler* Court thus made a strenuous effort to characterize its prior "special needs" cases as the exception rather than the rule." *Id.* at 517.

[132] 531 U.S. 32 (2000); *see* Kenneth Nuger, *The Special Needs Rationale: Creating a Chasm in Fourth Amendment Analysis,* 32 SANTA CLARA L. REV. 89, 97-98 (1992) ("Since noncriminal penalties are assessed against citizens detected in administrative searches, and since these searches are primarily intended to advance government policy rather than to criminally punish, the Supreme Court has had little difficulty embracing the constitutionality of administrative searches premised on decreasing levels of suspicion.").

[133] 532 U.S. 67 (2001) (striking down law where hospital employees and law enforcement cooperated to test pregnant women for drugs via urine samples and turn over results to police); *see* Christopher Mebane, Note, *Rediscovering the Foundation of the Special Needs Exception to the Fourth Amendment in* Ferguson v. City of Charleston, 40 HOUS. L. REV. 177, 209 (2003).

[134] The roots: The term "special needs" first appeared in Justice Blackmun's

*Ferguson*, set forth a "primary purpose" test: "What is the *primary purpose* to which the government intends to put the results of the search?"[135] If the answer is to collect evidence for law enforcement purposes, the "special needs" will not be applicable.[136] At first glance, the "primary purpose" test would appear to be the death knoll (under "special needs") for searches of probationer's homes where the primary purpose is to generate evidence for use in a criminal proceeding.[137] While criminal investigatory searches (i.e., FP1) would seem, at first glance, to fail in light of *Edmond* and *Ferguson*, routine (administrative) probationary searches (i.e., FP2) would likely survive, for they fit the original model of the "special needs" warrantless search.[138]

### *ii. A Return to* Griffin *After* Ferguson

While the general momentum of "special needs" seemed to be harnessed by *Edmunds* and *Ferguson*,[139] a lone footnote in

---

concurring opinion in *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring). Justice Blackmun agreed with the Court that there are "limited exceptions to the probable-cause requirement" in which reasonableness is determined by "'a careful balancing of governmental and privacy interests,'" but concluded that such a test should only be applied "in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *Id.* Interestingly, Justice Blackmun dissented in *Griffin* as he was the author of the concurrence that formed the basis for the "special needs" doctrine in *T.L.O.*

[135] Jonathon Kravis, Comment, *A Better Interpretation of "Special Needs" Doctrine After* Edmond *and* Ferguson, 112 YALE L.J. 2591, 2593-94 (2003) (emphasis added).

[136] *Id.*

[137] *See supra* Part I(ii)—basically, this type of search would be indicated in FP1; *see also* Roe v. Texas Dep't of Protective & Regulatory Servs., 299 F.3d 395 (5th Cir. 2002).

[138] *See supra* note 124 and accompanying text.

[139] *See* Mebane, *supra* note 133, at 209 ("For practitioners and administrators, *Ferguson* means that special needs search regimes must be insulated from law enforcement entanglement, at least to the extent that a policy or program becomes 'indistinguishable from the general interest in crime control.'"). *But see Ferguson*, 532 U.S. at 100 (Scalia, J., dissenting) ("But that is quite impossible, since the special-needs doctrine was developed, and is ordinarily employed, precisely to enable searches *by law enforcement officials* who, of course, ordinarily

*Ferguson* makes all the difference to our inquiry and returns the "special needs" analysis in the context of probationers directly back to *Griffin*.[140] Although lengthy, the text of "Footnote 15" is worth including in its entirety because of the Court's analysis in relation to the "special needs" doctrine and probationers:

> As THE CHIEF JUSTICE recently noted: "The 'special needs' doctrine which has been used to uphold certain suspicionless searches performed for reasons unrelated to law enforcement, is an exception to the general rule that a search must be based on individualized suspicion of wrongdoing." *Indianapolis v. Edmond*, 531 U.S. 32, 54 (2000) (dissenting opinion); see also nn. 16-17, *infra*. In *T.L.O*, we made a point of distinguishing searches "carried out by school authorities acting alone and on their own authority" from those conducted "in conjunction with or at the behest of law enforcement agencies." 469 U.S., at 341, n.7.
>
> The dissent, however, relying on *Griffin v. Wisconsin*, 483 U.S. 868 (1987), argues that the special needs doctrine "is ordinarily employe[d], precisely, to enable searches *by law enforcement officials* who, of course, have a law enforcement objective." *Post*, at 1300. Viewed in the context of our special needs case law and even viewed in isolation, *Griffin* does not support the proposition for which the dissent invokes it. In other special needs cases, we have tolerated suspension of the Fourth Amendment's warrant or probable-cause requirement in part because there was no law enforcement purpose behind the searches in those cases, and there was little, if any entanglement with law enforcement. See *Skinner*, 489 U.S. at 620-621; *Von Raab*, 489 U.S. at 665-666; *Acton*, 515 U.S., at 658. Moreover, *after* our decision in *Griffin*, we reserved the question whether "routine use in criminal prosecutions of evidence obtained pursuant to the administrative scheme would give

---

have a law enforcement objective."). I honestly cannot figure out what Justice Scalia means by this probation in the context of the history of the "special needs" doctrine. Scalia then cites to *Griffin*, *id.*, which is more the exception to the "special needs" doctrine than the rule, and does not explain how the doctrine was developed by law enforcement officials in any other context.

[140] *Ferguson*, 532 U.S. at 79 n.15.

> rise to an inference of pretext, or otherwise, impugn the administrative nature of the . . . program." *Skinner*, 489 U.S., at 621 n.5. In *Griffin* itself, this Court noted that "[a]lthough a probation officer is not an impartial magistrate, neither is he the police officer who normally conducts searches against the ordinary citizen." 483 U.S., at 876. Finally, we agree with petitioners that *Griffin* is properly read as limited by the fact that probationers have a lesser expectation of privacy than the public at large. *Id.* 874-875.[141]

"Footnote 15" seems to maintain the viability of the "special needs" test in the context of probationary searches and/or monitoring. Two primary, relevant themes are set forth:

> (1) The question left open: whether the "routine use in criminal prosecutions of evidence obtained pursuant to the administrative scheme would give rise to an inference of pretext, or otherwise, impugn the administrative nature of the . . . program" goes to the heart of the distinction between the two "Fact Patterns" set forth in Part I(ii). Given that the evidence being collected is for "routine use in criminal prosecutions," the question is left open as to FP1. FP2 seems to survive, and even flourish, under the "reigned in" view of "special needs" set forth in *Ferguson*, as it fits the original conception of "special needs."[142]
>
> (2) Next, the Court provides itself an "out" by providing that *Griffin* is a special, "special needs" case because "probationers have a lesser expectation of privacy than the public at large."[143]

---

[141] *Id.*

[142] *See supra* note 127 and 139 and accompanying text. A probation officer, conducting computer monitoring as part of the regular supervision of an offender, where evidence and information collected will be used administratively instead of for the "law enforcement" purpose of criminal prosecution, and getting a warrant every time a probation officer conducted a routine "home visit" would both qualify as impracticable.

[143] *See supra* note 134 and Part VIII(ii) related to the warrant requirement and "special needs." This diminished reasonable expectation of privacy is asserted in numerous contexts as the reason that a warrant is not necessary even to search a private home.

*Ferguson* basically separates *Griffin* from the rest of the cases that make up the "special needs" doctrine.[144] As such, and due to its continued viability in the "special needs" area for probationers in light of *Ferguson*, a detailed examination of *Griffin* continues to be necessary.

### *iii. Griffin v. Wisconsin*

On September 4, 1980, Joseph G. Griffin, a convicted felon, "was convicted in Wisconsin state court of resisting arrest, disorderly conduct, and obstructing an officer."[145] He was placed on probation.[146] One of the probation department's regulations, and thus one of the conditions of Griffin's probation permitted "any probation officer to search a probationer's home without a warrant as long as his supervisor approves and as long as there are 'reasonable grounds' to believe the presence of contraband—including any item that the probationer cannot possess under the probation conditions."[147]

In April 1983, while Griffin was on probation, a supervisor from the probation department received word from a local police detective that "there were or might be guns in Griffin's apartment."[148]

---

[144] *See Ferguson*, 532 U.S. at 79 n.15. The "rules" do not apply because Footnote 15 makes the "primary purpose" test inapplicable to the "special needs" analysis set forth in *Griffin* for probationers.

[145] Griffin v. Wisconsin, 483 U.S. 868, 870 (1987).

[146] *Id.* "Wisconsin law puts probationers in the legal custody of the State Department of Health and Social Services and renders them 'subject . . . to . . . conditions set by the court and rules and regulations established by the department.'" *Id.* (citation omitted).

[147] *Id.* at 870-71 (citing WIS. ADMIN. CODE HSS §§ 328.21(4), 328.16(1) (1981)).

> The rule provides that an officer should consider a variety of factors in determining whether "reasonable grounds" exist, among which are information provided by an informant, the reliability and specificity of that information, the reliability of the informant (including whether the informant has any incentive to supply inaccurate information), the officer's own experience with the probationer, and the "need to verify compliance with rules of supervision and state and federal law." HSS § 328.21(7) Another regulation makes it a violation of the terms of probation to refuse to consent to a home search. HSS § 328.04(3)(k).

*Id.* at 871.

The supervisor, who was unable to locate Griffin's regularly-assigned probation officer, went to Griffin's apartment accompanied by another probation officer and three plainclothes police officers.[149] Griffin answered the door, and the probation officers identified themselves and stated "that they were going to search his home."[150] A handgun was recovered during the search.[151]

"Griffin was charged with possession of a firearm by a convicted felon."[152] Griffin's motion to suppress the evidence was denied by the trial court, and he was convicted by a jury and sentenced to two years imprisonment.[153]

The Wisconsin Supreme Court affirmed Griffin's conviction and found the denial of suppression proper, holding that the probation officer had "reasonable grounds" based on the tip of the informant detective.[154] The United States Supreme Court, in a 5-4 opinion authored by Justice Scalia, agreed with the

---

[148] *Id.* Is not this statement really the same thing as simply saying, "There might be guns in Griffin's apartment."?

[149] *Id.* Apparently, the police officers were involved only to provide protection for the two probation officers.

[150] *Id.* The search was "carried out entirely by the probation officers under the authority of Wisconsin's probation regulation." *Id.*

[151] *Id.*

[152] *Id.* at 872. This possession charge is, itself, a felony. *Id.*

[153] *Id.* His conviction was affirmed by the Wisconsin Court of Appeals. *Id.*

[154] *Id.*

> On further appeal, the Wisconsin Supreme Court also affirmed. It found denial of the suppression motion proper because probation diminishes a probationer's reasonable expectation of privacy—so that a probation officer may, consistent with the Fourth Amendment, search a probationer's home without a warrant, and with only "reasonable grounds" (not probable cause) to believe that contraband is present. It held that the "reasonable grounds" standard of Wisconsin's search regulation satisfied this "reasonable grounds" standard of the Federal Constitution, and that the detective's tip established "reasonable grounds" within the meaning of the regulation, since it came from someone who had no reason to supply inaccurate information, specifically identified Griffin, and suggested a need to verify Griffin's compliance with state law.

*Id.*

Wisconsin Supreme Court's ruling that the search did not violate the Fourth Amendment; however, the Court rejected a "new principle of law . . . that any search of a probationer's home by a probation officer satisfies the Fourth Amendment as long as the information possessed by the officer satisfies a federal 'reasonable grounds' standard."[155]

The Court held that the search was constitutional because "it was carried out pursuant to a regulation that itself satisfies the Fourth Amendment's reasonableness requirement under *well-established principles*."[156]

The "well-established principles" Justice Scalia referred to was the "special needs" doctrine, which first peered up, like a gopher from a hole, in the Court's Fourth Amendment jurisprudence just two years earlier in *New Jersey v. T.L.O.*[157] Regardless, a bare majority held that, due to the "special needs" of probation, a warrant was not required to search the home of a probationer in light of the circumstances at issue in *Griffin*.[158]

The Court's holding, overall, that the search of a probationer, because of the "special needs" of supervising probationers generally, was "reasonable" for purposes of Fourth Amendment analysis, because "it was conducted pursuant to a valid regulation governing probationers."[159]

---

[155] *Id.*

[156] *Id.* at 873 (emphasis added); *see supra* note 124 and accompanying text. To call the "special needs" doctrine, especially in 1987, two years after its "birth," "well-established" is a stretch.

[157] New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring). *T.L.O.* seems strikingly different from *Griffin* as it related to the "high-stakes" world of a high school principal searching a bratty fourteen-year-old girl's purse for cigarettes. *Id.* at 328. The search did become somewhat "high[er]-stakes" as it was revealed later that the freshmen girl (T.L.O.) not only had cigarettes, but also a "a small amount of marihuana, a pipe, a number of empty plastic bags, a substantial quantity of money in one-dollar bills, an index card that appeared to be a list of students who owed T.L.O. money, and two letters that implicated T.L.O. in marihuana dealing." *Id.* at 328 (majority opinion). Okay, so she is not really a smart drug dealer, just a drug dealer. An interesting intersection between the law and popular culture occurred in 1985, with Motley Crue's smash hit remake of *Smokin' in the Boy's Room* released July 13, 1985 the same year as the Court's ruling in *T.L.O.* Obviously, 1985 was the crescendo year for smoking in high school bathrooms for both girls and boys.

[158] *Griffin*, 483 U.S. at 873.

This broad holding would indicate that if a state enacts a regulation governing offenders with a conviction for Internet-related child pornography that is facially valid under the Fourth Amendment, due to the "special needs" of supervising probationers, it would pass constitutional muster under *Griffin*.

Three factors call into question this seemingly simple conclusion. First, the holding was by a bare 5-4 majority.[160] Next, in *Knights*, the Court could have seemingly applied the "special needs" precedent set forth in *Griffin*, but instead chose to review the search of Knights' apartment under a general "reasonableness" standard.[161] Finally, an unfortunate (in both name and holding) Second Circuit ruling, *United States v. Lifshitz*[162] muddies the seemingly clear waters of applying the "special needs" doctrine to a warrantless probationary search of a home pursuant to a condition of probation.

### *iv. United States v. Lifshitz*

In early 2001, as part of an investigation related to the source of certain transmissions of child pornography, FBI agents visited the home of Brandon Lifshitz.[163] The Lifshitzs consented to a search of a computer located in the home and also cooperated with FBI agents by submitting voluntarily to interviews.[164] During the interviews, Lifshitz admitted that he had both downloaded and transmitted child pornography since the year 2000.[165]

---

[159] *Id.* at 880. "This conclusion makes it unnecessary to consider whether, as the court below held and the State urges, *any* search of a probationer's home by a probation officer is lawful when there are 'reasonable grounds' to believe contraband is present." *Id.* (emphasis added).

[160] *Id.* at 868. This may be becoming less relevant as Justice O'Connor joined this slight majority back in 1987 and her replacement, be it Judge Roberts or someone else will likely be more, not less, likely to affirm the holding in this case if applied to a future set of facts. The Justices dissenting in several written and joined dissents were Blackmun, Marshall, Brennan and Stevens. Obviously, only Justice Stevens remains on the bench from this group.

[161] *Knights*, 534 U.S. at 118.

[162] 369 F.3d 173 (2d Cir. 2004).

[163] *Id.* at 175. The Lifshitz household included Brandon, then thirty years old, his mother, sister and niece. *Id.*

Lifshitz was indicted for two counts of violating federal child pornography law.[166] Pursuant to a plea bargain, Lifshitz pled guilty to one count of receiving child pornography in exchange for the government's agreement to drop the remaining count.[167]

As a matter of right, defense counsel submitted a letter requesting that the court depart downward to a non-custodial sentence.[168] After hearing the evidence, Judge Patterson, the trial court judge, sentenced Lifshitz to three years probation rather than send him to prison.[169]

However, while deciding not to send Lifshitz to prison, the Judge expressly enumerated other requirements.[170] It seems clear that if this type of monitoring was not available to the court, the Judge may well have sentenced Lifshitz to prison.[171] It should be noted that the trial Judge imposed the additional probation condition "at the same time" he granted the ten-level downward departure which allowed Lifshitz to avoid prison.[172] This timing indicates that the Judge felt this type of monitoring was crucial if Lifshitz was not to be incarcerated.[173]

---

[164] *Id.*

[165] *Id.* Brandon's mother "corroborated this account, indicating that she had observed him examining these materials on the computer and repeatedly requested that he delete them." *Id.* It is clear that this is not exactly the Walton's, looking at child porn with Mom looking on. The court notes: "The history of [Brandon's] past relationships was not, however, reassuring. As a teenager, he had initiated an incestuous liaison with his sister, and he had, more recently, pursued a correspondence over the Internet with an 18-year-old woman in Michigan to whom he ultimately paid a visit." *Id.* at 176.

[166] *Id.* at 175. "The first count alleged that he had 'unlawfully, willingly, and knowingly received [on his computer] child pornography . . . which had traveled in interstate commerce,' and the second stated that he had also 'unlawfully, willingly, and knowingly distributed child pornography . . . in interstate commerce.'" *Id.*

[167] *Id.* at 176.

[168] *Id.* Defense's request for "downward departure" was based on the claim that "Lifshitz's capacity was diminished at the time of the offense because he lacked the ability to control behavior that he knew was wrong." The defense entered three letters prepared by psychiatrists who interviewed Brandon. *Id.*

[169] *Id.* at 177. Judge Patterson stated: "I think the most important thing for the defendant is continued treatment and I don't think that for the variety of psychological problems that he has, not the least of which is his problem with attraction to children under the age of 18, . . . sentencing to prison will accomplish that objective." *Id.*

[170] *Id.*

The relevant probation condition at issue in Lifshitz's appeal reads:

> [T]he defendant shall consent to the installation of systems that will enable the Probation office or its designee to monitor and filter computer use on a regular or random basis and any computer owned or controlled by the defendant. The defendant shall consent to unannounced examinations of any computer equipment owned or controlled by the defendant which may result in the retrieval and copying of all data from the computer and any internal or external peripherals and may involve removal of such equipment for the purpose of conducting a more thorough investigation.[174]

Unlike the Supreme Court rulings in *Griffin* and *Knights*, the Second Circuit, in *Lifshitz*, dealt specifically with a particular condition of probation: "computer monitoring . . . imposed upon a probationer"[175] and whether the condition "infringes upon his right to be free of unreasonable searches."[176] As such, the facts in *Lifshitz* are closer in several respects to the fact pattern set forth in Part I(ii)(2), *supra*.

---

[171] *Id.* "*At the same time* as it granted this ten-level downward departure, the court imposed certain probation conditions, one of which underlies Lifshitz's appeal." *Id.* (emphasis added).

[172] *Id.*

[173] It also seems that if the defense did not intend to comply with the conditions of probation they could have instead asked the judge to incarcerate Lifshitz. Defense counsel did "vigorously object[] to this condition;" however, they did not instead choose incarceration. *Id.*

[174] *Id.*

[175] *Id.* at 175. In this instance a probationer with a previous conviction for Internet-related Child Pornography. *Id.* at 173.

[176] *Id.* at 175. Other sections of this article will deal with the initial question as to whether this condition is "imposed" upon a probationer when the alternative is jail. *See supra* Part III.

The ruling in *Lifshitz* is straightforward. The court "holds that the 'special needs' of a probation system may render a computer monitoring reasonable" generally under the Fourth Amendment; however, in this particular case the specific monitoring condition "may be overbroad."[177] Due to the possible overbreadth of the condition at issue in *Lifshitz*, the Second Circuit remanded the case to the district court for the "imposition of a condition consistent with this opinion."[178]

The *Lifshitz* court, after expressly holding that the "special needs" doctrine should apply, ruled in a manner that totally eviscerated the reality of what probation is and why probation officers search probationer's dwellings or conduct home visits in the first place. Stated differently, the Second Circuit, in applying the "special needs" doctrine totally forgot about what makes supervising probationers "special" in the first place and why it is treated distinctly under the Supreme Court's Fourth Amendment jurisprudence.[179]

To evaluate the constitutionality of the type of computer monitoring at issue in *Lifshitz*, the Second Circuit sought to "discern[] the kind of search to which computer monitoring bears the closest resemblance."[180] The court concluded that computer monitoring "bears the closest resemblance" to drug testing in the special needs context.[181]

While drug testing may be analogous in certain ways,[182] there are several distinctions, both theoretical and technological, which question the value of the court's use of this analogy.[183]

---

[177] *Id.* at 175. The holding that this type of monitoring is "overbroad" can be viewed as somewhat inconsistent with the Second Circuit's ruling, two years earlier, in *United States v. Sofsky*, 287 F.3d 122 (2d Cir. 2002).

[178] *Id.* at 175.

[179] *See supra* Part VI(i).

[180] *Id.* at 182. ("Considering the contours of special needs searches is instructive as to the permissible extent of such searches under the Fourth Amendment."). *Id.*

[181] *Id.* The court noted that "[t]he government insisted in both its brief and at oral argument that drug testing conditions constituted an 'apt analogy to the computer monitoring condition . . . .'" *Id.*

[182] *Id.* at 189. "As we have previously observed . . . there is a high rate of recidivism among sex offenders like drug users." *Id.* (citation omitted).

The court speaks specifically to the degree of "narrow tailoring" available in computer monitoring:

> In order to comply with the requirements of the Fourth Amendment, the monitoring condition must be narrowly tailored, and not sweep so broadly as to draw a wide swath of extraneous material into its net. Drug testing procedures provide the relevant point of comparison here. As the Supreme Court has consistently emphasized, urinalysis and other means of determining drug use should be precisely targeted to ascertain only whether an individual has used illegal substances.[184]

In other words, the court believes that monitoring should be "narrowly tailored" in a manner that the probation officers would somehow monitor or examine a computer and only learn whether the probationer has looked at child porn and learn nothing else about their viewing habits or history.[185] While it may be possible to draw blood or urine and test it in a manner that only a gives a "positive" or "negative" as to whether marijuana (THC) or cocaine is present, no technology currently exists that will simply give a "positive" or "negative" as to whether an offender viewed or downloaded child porn without providing additional, and in many cases, "extraneous[,] material[s]" to the officer monitoring the offender.[186] In a probation setting, the "extraneous materials" are relevant as the goal of supervised release is to determine how the individual is living, not necessarily whether they are breaking particular criminal laws.[187] Further, if such technology did exist, while it would be extremely valuable in performing forensic computer examinations, because of the goals of supervised release, a simple yes or no to the question of whether child pornography is present on the computer does not fully meet the needs of probation. Further, the court is also seemingly mixing apples and oranges by interchanging the concepts of "testing" and "monitoring."

---

[183] *But see id.* at 182 (The government agreed that this was a proper analogy).

[184] *Id.* at 190.

[185] *Id.*; *see* Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193 (2005).

> Such close tailoring analysis is, however, inappropriate in the Fourth Amendment context, which, instead of barring governmental intrusions, requires only that the intrusion be reasonable. This is to say that reasonableness is a more forgiving concept than a least intrusive means analysis allows. In accordance with that mandate, the means need be only reasonably related to the justification for the intrusion.

*Id.* at 215.

[186] *But see infra* Part IX.

In *Lifshitz*, the court states that the computer monitoring "must . . . remain narrow."[188] In identifying the relation of computer monitoring to other types of "special needs" searches, the court identifies that, for permissible warrantless testing the following three requirements must be met:

1. Reduced expectation of privacy on the testing subject;

---

[187] *See supra* note 21 and accompanying text. This distinction, between revealing only criminal activity and "extraneous information" or "information about perfectly lawful activity," while not directly relevant in the probation context, has been considered twice recently by the United States Supreme Court. *See* Illinois v. Caballes, 125 S. Ct. 834 (2005); Kyllo v. United States, 533 U.S. 27 (2001).

> Accordingly, the use of a well-trained narcotics-detection-dog, one that "does not expose noncontraband items that otherwise would remain hidden from public view," during a lawful traffic stop, generally does not implicate legitimate privacy interests. In this case, the dog sniff was performed on the exterior of respondent's car while he was lawfully seized for a traffic violation. Any intrusion on respondent's privacy expectations does not rise to the level of a constitutionally recognized infringement.
>
> This conclusion is entirely consistent with our recent decision that the use of a thermal-imaging device to detect the growth of marijuana in a home constituted an unlawful search. Critical to that decision was the fact that the device was capable of detecting lawful activity—in that case, intimate details in a home, such as "at what hour each night the lady of the house takes her daily sauna and bath." The legitimate expectation that information about perfectly lawful activity will remain private is categorically distinguishable from respondent's hopes or expectations concerning the nondetection of contraband in the trunk of his car. A dog sniff conducted during a concededly lawful traffic stop that reveals no information other than the location of a substance that no individual has any right to possess does not violate the Fourth Amendment.

*Caballes*, 125 S. Ct. at 838 (citations omitted).

[188] *Lifshitz*, 369 F.3d at 189.

2. Random or otherwise non-discretionary implementation of the testing program; and
3. Narrowness of the scope of testing.[189]

While this might appear to be an accurate test for suspicionless drug testing in the areas of education[190] and certain types of employment,[191] the application of these requirements in a probation setting is misplaced. Although, in the context of probation No. 1, above, will always be met, the second two parameters have nothing to do with the supervisory activities of a probation department and are misplaced within the parameters of why the "special needs" doctrine was created, and applied to probation supervision, to begin with.[192]

### *v. The Special Needs Approach—Continued Viability*

The *Lifshitz* anomaly aside,[193] the "special needs" doctrine remains viable as a relevant analysis for court's to apply in reviewing the search and/or monitoring of a probationer's computer.[194] Using "special needs" as the basis for reasonableness under *Griffin* appears strongest when the government actors are probation officers and the search and/or monitoring is pursuant to an otherwise valid probation regulation.[195] This is most akin to FP2.[196] The validity of "special needs" weakens in FP1 because of both the level of individualized suspicion and the fact that these searches are in conflict with the two primary bases of "special needs," that the search be for a non-law enforcement purpose and obtaining a warrant would be "impracticable."[197]

---

[189] *Id.* at 183.

[190] *See, e.g.,* Bd. of Educ. v. Earls, 536 U.S. 822 (2002); Vernonia Sch. Dist. v. Acton, 515 U.S. 646 (1995).

[191] *See, e.g.,* Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602 (1989); Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656 (1989).

[192] *See supra* Part VI.

[193] An additional reason that *Lifshitz* seems to be an anomaly is that it is what appears to be a facial Fourth Amendment challenge. In other words, Lifshitz has not been subject to a particular search for a court to review, instead, he is challenging the general validity of the probation condition prior to any actual search being conducted pursuant to it.

[194] *See supra* Part VI.

[195] *See supra* note 24.

[196] *See supra* part I(ii)(2).

## PART VII. PLACING PROBATIONARY COMPUTER SEARCHES OF SEX OFFENDERS IN THE HISTORICAL CONTEXT OF THE FOURTH AMENDMENT: GENERAL WARRANTS, "WRITS OF ASSISTANCE" AND THE "RIGHT TO BE LEFT ALONE"

Gauging modern search and seizure conundrums in the context of James Otis[198] and the oppressive English practices of general warrants[199] and "writs of assistance" is an important return to the basic premises that underlie our Fourth Amendment.[200] George C. Thomas, III was correct in his statement "[h]istory has probably been used (and misused) more frequently in seeking to understand the Fourth Amendment than all other criminal procedure rights combined."[201] The general story of Otis, and his dramatic oratory that sparked the birth of "child Independence"[202] is well-documented in Fourth Amendment lore.[203]

---

[197] *See supra* note 133 and accompanying text.

[198] *See generally*, Thomas K. Clancy, *Introduction to James Otis Lectures*, 74 MISS. L.J. 627, 628-29 (2004) ("Otis would become one of the greatest patriots our country has ever known. Though eventually reduced to insanity and ultimately silenced by a bolt of lightning, James Otis will forever remain first among America's Fourth Amendment advocates.").

[199] Sundby, *supra* note 7, at 511 ("Not surprisingly, the Court's growing receptivity to the idea that a search or seizure can be "reasonable" outside the traditional requirements of the Warrant Clause has had important ramifications. For our purposes of thinking about a rebirth of concern over general warrants, . . . .").

[200] *See* John M. Burkoff, *The Fourth Amendment and Terrorism*, 109 PENN ST. L. REV. 911, 912 (2005) ("In short, the protections enshrined in the Fourth Amendment are important not only because they are the law, and not only because they are part of our Bill of Rights, but also because they are a vital and significant part of our history, our self-identity, our democracy, and our national culture.").

[201] George C. Thomas, III, *Time Travel, Hovercrafts, and the Framers: James Madison Sees the Future and Rewrites the Fourth Amendment*, 80 NOTRE DAME L. REV. 1451, 1460 (2005).

[202] NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 59 (1937).

[203] *See generally*, Alison L. LaCroix, *"Bound Fast and Brought Under the Yoke":*

I maintain that probationary computer searches (and monitoring) can be distinguished (at least conceptually) from the highly-despised general warrants[204] and "writs of assistance" of Otis's times based on two primary bases: (1) legal status of probationer; and (2) searches are not directly pursuant to legislative action.[205]

---

*John Adams and the Regulation of Privacy at the Founding*, 72 FORDHAM L. REV. 2331, 2350 (2004); David E. Steinberg, *An Original Misunderstanding: Akhil Amar and Fourth Amendment History*, 42 SAN. DIEGO L. REV. 227, 260-61 (2005). *See also* Scott E. Sundby, *Protecting Citizen "Whilst He is Quiet": Suspicionless Searches, "Special Needs" and General Warrants*, 74 MISS. L.J. 501, 538-43 (2004) (discussion of Otis's argument against "writs of assistance' as well as full-text of speech that author correctly asserts "is a speech that every student of criminal procedure should be exposed to at least once"); United States v. Rabinowitz, 339 U.S. 56, 69-72 (1950) (Frankfurter, J., dissenting) (detailing Otis's argument as a "clue" to the meaning and scope of Fourth Amendment), *overruled on other grounds by*, Chimel v. California, 395 U.S. 752, 768 (1969).

> In February 1761, Otis delivered his famous speech against the Writs of Assistance in the council chamber at Boston's Old State House. He spoke for four hours before a penal of judges including Lieutenant Governor and chief Justice Thomas Hutchinson. In those four hours lit the spark of revolution in his compatriots' hearts. John Adams, who was present when Otis delivered his speech, later stated, "Mr. Otis' oration breathed into this nation the breath of life . . . then and there was the first scene of the first act of the opposition to the arbitrary claims of Great Britain . . . American independence was then and there born."
>
> In his speech Otis argued that the British writs were not constitutional But his arguments transcended the issues of common law. He maintained that the writs were in violation of natural law, elevating the issues at hand to political and philosophical levels. He even spoke of human rights and used the speech to denounce slavery.
>
> Though no copies of the speech have survived, those who heard it described it as "eloquent," "impassioned," "monumentous," and the product of "conclusive reasoning." Adams did take notes during the speech and 60 years later attempted to reconstruct what he could of Otis' oration. He later said, "Otis was a flame of fire" and that he had "a prophetic glance of his eyes into futurity."x" Otis even made reference to "my country" when referring to the colonies, marking the first instance of anyone conceiving of a nation separate and independent from the crown.

James "Patriot" Otis, *available at* http://www.otismac.com/HISJamesThePatriot.htm (last visited Aug. 23, 2005) [as with anything dating back to 1761, certain details and exactness of quotes differs in the passage included on the www.otismac.com website from other sources I have read and cited herein].

[204] *See supra* note 80 and accompanying text for contract analysis applied to dismiss what was basically a "general warrant" argument.

[205] "[T]he history of the [Fourth] Amendment suggests that legislative abuse

### *i. Legal status of the Child Pornographer/Probationer*

Otis's oft-quoted words: "A man's house is his castle—and *[whilst] he is quiet,* he is as well guarded as a prince in his castle."[206] While the context of the search at issue is in the home,[207] an individual convicted of Internet-related child pornography who is on probation instead of being incarcerated is hardly the type of "quiet" citizen Otis likely envisioned.[208] Further, the idea of "retreat[ing] thence" into ones "castle' is somehow lost in the context of the pedophile hooked up to almost instantaneous international access via high-speed Internet connection.[209] The idea of the home as a

---

was precisely the evil the Fourth Amendment was intended to eliminate. In stark contrast, the Framers did not fear that judicial officers . . . posed a serious threat to Fourth Amendment values." Illinois v. Krull, 480 U.S. 340, 364 (1987) (O'Connor, J., dissenting). "The distinction drawn between the legislator and the judicial officer is sound. The judicial role is particularized, fact specific, and non-political." *Id. But see* CASS R. SUNSTEIN & RICHARD A. EPSTEIN (editors), THE VOTE—BUSH, GORE & THE SUPREME COURT 1-266 (2001) (for a series of eleven essays, and additional commentary, on the role of the United States Supreme Court (both positive and negative views) in the 2000 presidential election and the resulting case, *Bush v. Gore*, 531 U.S. 98 (2000) (per curiam)); Editorial, *Judge Roberts's Record,* WASH. POST, July 25, 2005 at A18 (one example of the highly politicized nature of United States Supreme Court nomination and confirmation).

[206] James Otis, *Against the Writs of Assistance* (1761), reprinted in M.H. SMITH, THE WRITS OF ASSISTANCE CASE 548, 554 (1978) (emphasis added). I have to mention and thank my colleague David Case for humorously reminding me of the irony in the "whilst he is quiet" language. Sometimes when people are too quiet is when you must worry about them the most.

[207] *See supra* note 14 and accompanying text.

[208] The Seventh Circuit seemed to reject a general warrant argument on behalf of a probationer generally based on the fact that the offender could be incarcerated which would be more restrictive than even a general warrant. *Barnett*, 415 F.3d at 692.

> Barnett argues that to enforce such a blanket consent would invite abuse—for what if the probation officer decided to camp in Barnett's home and search him every five minutes? This argument ignores not only the alternative facing Barnett—the greater deprivation of privacy entailed by most forms of imprisonment, though this depends on the specific rules and conditions of the particular prison . . . .

*Id.*

[209] *See* Christa M. Book, *Do You Really Know Who is On the Other Side of Your Computer Screen? Stopping Internet Crimes Against Children*, 14 ALB. L.J.

"sanctuary"[210] may be increasingly misplaced in a technological time where an individual is physically and geographically in their home, but virtually and digitally "out in public."[211]

Another Fourth Amendment and privacy standby, the unenumerated, but ever-popular, right "to be left alone"[212] is also problematic for individuals on probation. Can a sex offender who is on probation, who could be incarcerated instead, really expect "to be left alone"?[213]

---

SCI. & TECH. 749, 750 (2004) ("Pedophiles have easier access to children in the age of the Internet; they can literally enter a child's home and not be detected.").

[210] *See, e.g.*, Segura v. United States, 468 U.S. 796, 810 (1984) ("The sanctity of the home is not to be disputed."); Welsh v. Wisconsin, 466 U.S. 740, 750 (1984) (noting "sanctity of the home").

[211] A full discussion of this distinction is outside the scope of this article.

[212] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890); *see also* THOMAS M. COOLEY, COOLEY ON TORTS 29 (2d ed. 1888) ("The right to one's person may be said to be a right of complete immunity: to be left alone.") (in the context of assault and battery, not government searches); Daniel Yeager, *Overcoming Hiddenness: The Role of Intentions in Fourth Amendment Analysis*, 74 MISS. L.J. 553, 554-55 (2004).

[213] It seems increasingly unrealistic. *See, e.g.*, Jennifer B. Siverts, *Punishing Thoughts Too Close to Reality: A New Solution to Protect Children from Pedophiles*, 27 T. JEFFERSON L. REV. 393 (2005).

> Creative measures affecting pedophiles have been implemented at each stage of the criminal justice process. At the trial stage, Federal Rules of Evidence 414 and 415 allows evidence of past, similar acts of child molestation to be admitted in criminal and civil cases where the accused faces a child molestation allegation. This renders prosecution much easier. At the sentencing stage, some states offer or even require as a condition of probation, administration of the drug Depo-Provera, which renders a person impotent, thereby eliminating the threat repeat sex offenders pose. Once an offender is released from treatment or prison, he then must register as a convicted sex offender with the local police department. These listings are available to the public and are used by the police to investigate future cases of crimes against children.

*Id.* at 399; *see also* Doron Teichman, *Sex, Shame, and the Law: An Economic Perspective on Megan's Laws*, 42 HARV. J. ON LEGIS. 355 (2005).

> The legal system does not function in a vacuum. Some acts that are governed by legal rules are also governed by social norms. In many cases, these social norms are enforced by a set of non-legal sanctions, which include internal sanctions such as guilt and external sanctions such as the refusal to interact with an offender.

*Id.* at 355.

### *ii. "Search" Not Pursuant to Legislative Action*

"[L]egislative abuse was precisely the evil the Fourth Amendment was intended to eliminate. In stark contrast, the Framers did not fear that judicial officers, the state actors at issue in *Leon*, posed a serious threat to Fourth Amendment values."[214] The analysis here is somewhat skewed. In many cases what is being challenged is law enforcement action taken pursuant to legislative enactment that is imposed[215] and applied by the judiciary. Otis's words relating to particularity and its effect on the manner in which the public is intruded upon are relevant:

> In the first place, may it please your Honors, I will admit that writs of one kind may be legal; that is, special writs, directed to special officers, and to search certain houses &c. specially set forth in the writ, may be granted by the Court of Exchequer at home, upon oath made before the Lord Treasurer by the person who asks it, that he suspects such goods to be concealed in those very places he desires to search.[216]

Here, the comparison must be done by analogy, but it remains relevant. Terms of probation subsequent to a conviction are dissimilar to a general warrant that subjects all people equally to governmental intrusion without any individualized suspicion.

The judicial imposition of such conditions[217] upon a cer-

---

> SORNLs, commonly known as Megan's Laws, reflect a significant change in the landscape of American criminal law. In general, these laws require convicted sex offenders who are released into the community to register as offenders and provide for some level of public notification as to the presence of a sex offender in a community. Currently, all fifty states and the District of Columbia have enacted their own SORNLs.

*Id.* at 378.

[214] Illinois v. Krull, 480 U.S. 340, 364 (1987) (O'Connor, J., dissenting).

[215] *See supra* Part III. My view is that they are not imposed but "bargained for" and waived via consent, assuming the consent is otherwise valid.

[216] *Krull*, 480 U.S. at 364-65 (O'Connor, J., dissenting) (citing 2 WORKS OF JOHN ADAMS 523 (C. Adams ed., 1850)).

[217] *See supra* note 213 and accompanying text.

tain sub-set of people who have been convicted of a heinous crime against children and are, therefore, subject to continuous and legitimate governmental scrutiny during the term of their probation, is far removed from the general warrants which prompted both Otis's ire and the American Revolution.

## PART VIII. PROPOSAL OF MANDATORY "WARRANT-PREFERENCE" MODEL REGARDLESS OF OCCUPANT'S REASONABLE EXPECTATION OF PRIVACY APPLYING "PRACTICABILITY" AS CONTROLLING STANDARD

Under either the "reasonableness" track (that the search at issue is "reasonable" under the applicable balancing) or "special needs" track (that the "special needs" exception applies and therefore the Fourth Amendment is not violated), the first prong of the Fourth Amendment: "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" (Reasonableness clause),[218] appears satisfied.[219] However, the second prong, "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation" (Warrant clause), becomes problematic when the search at issue takes place in the home,[220] and obtaining a warrant is not "impracticable."[221]

---

[218] U.S. CONST. amend. IV.

[219] *See supra* parts V & VI.

[220] *See supra* note 14 and accompanying text. This is a "constant" in both factual scenarios (FP1 & FP2).

[221] This is the case in FP1. *See supra* Part I(ii)(1).

> There is nothing about the *status* of probation that justifies a special exception to the warrant requirement under these circumstances. If in a particular case there is a compelling need to search the home of a probationer without delay, then it is possible for a search to be conducted immediately under the established exception for exigent circumstances. There is no need to create a separate warrant exception for probationers. The existing exception provides a probation agent with all the flexibility the agent needs.

Griffin v. Wisconsin, 483 U.S. 868, 885 (1987) (Blackmun, J., dissenting).

### *i. Reasonableness and the Warrant Clause in Context of Warrantless Probationary Searches*

Fortunately, I am not required to totally "re-invent the wheel" with regards to the meaning of the "reasonableness" clause of the Fourth Amendment due to Thomas K. Clancy's exhaustive research and scholarship on the subject.[222] For the purposes of this section, I will follow the five principal models set forth in Professor Clancy's article generally.[223] I would maintain, given that the search at issue in this analysis always involves intrusions into an individual's home,[224] the warrant preference rule should apply. In the context of routine probation home-visits and the like, (i.e., FP2), the fact that a warrant is not needed is settled law.[225]

However, in FP1, where there is the requisite level of individualized suspicion, the fact that the "dwelling" is the home should override the diminished reasonable expectation of privacy, the warrant preference model should apply, and a warrant should be obtained. Similar to my analysis in the context of waiver, I believe that the protections of the Fourth Amendment either do or do not apply. Until the United States Supreme Court states affirmatively that a probationer has no reasonable expectation of privacy[226] given that they could instead be incarcerated, the protections of the Amendment apply, and, when the target is a private home, a warrant should be secured. Obviously, the facts at hand may indicate a separate basis for a warrantless intrusion into the dwelling (i.e., exigency, "hot-pursuit", etc.), but, simply based on the fact that the individual is on probation, and nothing more, the "castle-doctrine" should apply and the warrant-preference model should govern.[227] Also, given the advantageous "fluid" nature of the Fourth Amendment generally, the relevant factor of probation,[228] the high recidivism rate of child pornography offenders,[229] and similar factor, will be taken into account in the calculation of probable cause. However, a warrant should still be required to enter a home.[230] Any home.[231]

---

[222] *See* Thomas K. Clancy, *The Fourth Amendment's Concept of Reasonableness*, 2004 UTAH L. REV. 977 (2004).

[223] *Id.* at 978 ("The Court chooses from at least five principal models to measure reasonableness: the warrant preference model, the individualized suspicion model, the totality of the circumstances test, the balancing test, and a hybrid model that gives dispositive weight to the common law.").

[224] *See supra* Part I(i).

[225] This is due to the routine standard operating procedures of federal and state probation agencies or the fact that it would amount to a "strong governmental interest" (supervision of probationers). *See Clancy*, *supra* note 223, at 1029. Further, remember that even if a Fourth Amendment violation should occur, the exclusionary rule would not apply in the context of FP3. *See supra* note 26 and accompanying text.

[226] *See* United States v. Knights, 534 U.S. 112, 120 n.6 (2001) ("We do not decide whether the probation condition so diminished, or completely eliminated, Knights' reasonable expectation of privacy . . . ."). The idea of "diminished" or "eliminated" reasonable expectations of privacy seems like a double-dipping of the same test. Isn't this just the same way of saying, "until we decide that a

---

probationer's expectation of privacy is unreasonable." Under *Knights*, until they say it is "unreasonable" or "diminished" or "eliminated," the Fourth Amendment would appear to continue to apply. It either meets the lowest threshold of reasonableness or it does not.

[227] I would assert that the "warrant preference rule" is the correct approach when the target of the search involves intrusion into a private home. *See* Clancy, *supra* note 223, at 1028-29 ("Next in order is the warrant preference rule. That rule does not have general applicability; it is, instead, limited to intrusions into buildings, a person's body, and speech-related concerns.").

[228] *See supra* Part II.

[229] United States v. Lifshitz, 369 F.3d 173, 189 (2d Cir. 2004) ("[T]here is a high rate of recidivision among sex offenders.").

[230] *See* Griffin v. Wisconsin, 483 U.S. 868, 882 (1987) (Blackmun, J., dissenting).

> My application of the balancing test leads me to conclude that special law enforcement needs justify a search by a probation agent of the home of a probation on the basis of a reduced level of suspicion. *The acknowledged need for supervision, however, does not also justify an exception to the warrant requirement, and I would retain this means of protecting a probationer's privacy.* Moreover, the necessity for the neutral check provided by the warrant requirement is demonstrated by this case, in which the search was conducted on the basis of information that did not begin to approach the level of "reasonable grounds."

*Id.* (emphasis added).

[231] Obviously, other valid exceptions to the warrant requirement could still apply (i.e., exigency, "hot-pursuit").

### *ii. "Special Needs" Doctrine and the Warrant Clause in Context of Warrantless Probationary Searches*

While I agree with Maclin, Sundby, and many others that the special needs doctrine is both incoherent[232] and policy driven,[233] I must heed to the adage "it is easier to criticize than construct."[234] If the "special needs" doctrine is to continue to exist, the Court should continue the trend in *Edmund* and *Ferguson* and reign the doctrine back to its original "root" application.[235] Like other exception doctrines, such as the "pat-and-frisk" doctrine set forth under *Terry v. Ohio*[236] and the application of the "secondary effects" doctrine in the First Amendment,[237] the "special needs" doctrine has evolved into an increasingly unsound, incoherent, and over-expansive doctrine that has strayed far from its intended application.[238]

Returning to the "roots" of the "special needs" doctrine, the analysis is straightforward within the context of our two stated factual scenarios.[239] Given that the "special needs" doctrine has generally applied where the warrantless search is for a non-law enforcement purpose and obtaining a warrant would be impracticable, FP2, the activities of probation officers in their normal duties, fits nicely into the model, even in light of the "tempered" "special needs" doctrine post-*Edmunds* and *Ferguson*.[240] In this fact pattern, the primary purpose of the search and/or monitoring activity is to gauge compliance with probation conditions. Any evidence gathered is to be used at an administrative probation revocation hearing; the "primary purpose" is not general law enforcement. It is impracticable to obtain a warrant to do every home visit where the search and/or monitoring is part of the regularly scheduled procedure of the probation department and not based on individual suspicion of a particular probationer.

---

[232] *See supra* note 128 and accompanying text.

[233] Sundby, *supra* note 7, at 551 (detailing special needs doctrine as allowing the court to act as a "policy magistrate").

[234] Clancy, *supra* note 223, at 1043.

[235] *See supra* note 125 and accompanying text.

[236] 392 U.S. 1 (1968). *See generally* Stephen A. Saltzburg, Terry v. Ohio: *A Practically Perfect Doctrine,* 72 ST. JOHN'S L. REV. 911, 911 (1998).

[237] *See* Marc M. Harrold, *Stripping Away at the Constitution: The Increasingly Paternal Voice of Our 'Living' Constitution*, 32 U. MEM. L. REV. 403, 431 (2002) ("Possibly the boldest step of all, taken by the United States Supreme Court in *Pap*'s was the expansion of the 'secondary effects' doctrine to the point of an absolute ban, in this case, of nude dancing.") (without any ample alternative).

[238] *See supra* note 128 and accompanying text.

[239] *See supra* part I(ii)(1 & 2).

[240] In a more limited manner, see Chandler v. Georgia, 520 U.S. 305 (1995); *see also supra* notes 132-36 and accompanying text.

However, in FP1, where the probation or other law enforcement agency is acting on some level of individualized suspicion to obtain evidence for an admitted law-enforcement purpose (e.g., as evidence in a criminal prosecution), the special needs doctrine should not apply. The sticking point, of course, is "Footnote 15" set forth in *Ferguson*.[241] The fact that probationers clearly have a "lesser expectation of privacy than the public at large" is relevant in the "fluid" determination of probable cause to issue a warrant. However, it is not valid as a blanket determination to dismiss the core-values of special needs: non-law enforcement basis or impracticability.[242]

The "purpose" is not affected per se by the diminished expectation of privacy, nor does this diminished expectation of privacy create a general presumption of impracticability.

## PART IX. PRACTICAL APPLICATIONS OF COMPUTER MONITORING

In this section, it becomes necessary to depart from the collective analysis of computer forensic searches and probationary computer "monitoring" and focus exclusively on the latter. The field of practical methods for computer forensic data recovery and analysis generally is well-documented, and a full discussion is outside the scope of this article.[243] However, the practice of probationary computer monitoring is not as well developed in legal and technical literature

---

[241] *See supra* note 140 and accompanying text.

[242] *See supra* note 134 and accompanying text.

[243] An excellent resource is the *"CCIPS Manual": Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, published by the Computer Crime and Intellectual Property Section, (CCIPS) Criminal Division, U.S. Department of Justice (July 2002), *available at* http://www.usdoj.gov/criminal/

This section will provide an *overview* of the existing technology relevant to computer monitoring in the probation context and of the existing practical approaches (including a brief overview of prominent software) currently being utilized by probation agencies.[244] Although this article deals specifically with computer monitoring of a probationer with a previous conviction for one type of sex offense (Internet-related child pornography) the information in this section deals with monitoring sex offender computers generally within the context of probation.

Probationary computer monitoring is part of an overall goal of containment.[245] As such, it is distinguishable from traditional computer forensics. The primary distinction is that computer forensics looks backwards in time to collect evidence to convict an individual for a particular offense, while computer management, including computer monitoring, looks forward to determine the manner in which an individual is living while on probation and whether this manner is consistent with the terms of probation.[246]

---

cybercrime/s&smanual2002.htm (last visited July 30, 2005).

[244] A complete examination of these topics is extensive and outside the scope of this brief section. A portion of this material stems from materials (PowerPoint slides and accompanying documents) prepared by Dr. James L. Tanner for his presentation at the University of Mississippi School of Law on February 16, 2005 (materials on file with author).

[245] Containment is (1) an individual who has admitted the compulsion or deviant act(s); (2) an individual who actively takes steps to reduce the destructive behavior; (3) an individual who has external support for continued resistance to destructive urges; and (4) an individual who recognizes risk and has a plan for dealing with it. Early attempts to deal with probationers who had used computers to victimize children was in the form of an outright deprivation towards either all computers generally or any computer with Internet access. As this was an outright deprivation, and not a "search" or "monitoring program" the Fourth Amendment did not apply. However, the resulting "Circuit-split" that emerged is indicative and instructive as to how different Circuits, and different courts, view computer restrictions in the probation context generally. *See infra* Part X.

[246] Computer management only looks backwards in order to gain information as to what to watch for in the future.

### a. *Management/Monitoring Software*

There are four basic approaches to existing management (monitoring) software.[247] The first is "filtering software." Filtering software blocks access to certain websites and logs a user's usage. Next, there are two types of "system resident" approaches. The first type requires that the probation official actually be at the probationer's computer in order to monitor the usage (Type I). There is also "system resident" software that e-mails reports back to the probation official (Type II). The official does not physically have to be at the offender's computer. The last type is the "forced gateway" software that can be reviewed remotely by probation officials.[248] The next section details three management forensic "models" distinguished primarily on whether the "managing" forensic examiner is employed directly by the government (probation official), privately by the offender, or a combination of the two, as part of their court-ordered rehabilitation/treatment (Tx) regime.

---

[247] Two of the primary goals of monitoring software is to detect patterns of pornography viewing (or "TRAPS") and identify "Red Flags." "TRAPS": (T)hemes—the content or interest areas of pornography viewing and/or usage; what proportion of times was spent on which type(s) of material; (R)atio—the proportion of "porn surfing" to total Internet/computer usage; (A)mount—the total amount of time spent surfing pornography sites; (P)ace—the speed with which one moves from site to site and image to image; and (S)ession—the length of the average sessions, frequency of surfing, how deeply into the various sites the offender delved? There are several "Red Flags". The seven major "Red Flags" are:

1. Nude or sexual pictures of the offender;
2. Nude or sexual pictures taken by the offender;
3. Images of a victim;
4. "Trophy" materials from victims;
5. Beastiality images in any significant number;
6. Non-consensual or coercion sites (e.g., www.bangbus.com); and
7. Sexually explicit stories written by the offender.

Other relevant monitoring technology that exists outside the four primary software monitoring classifications (include "WHOIS" (a free web-based tool that enables officers to look up a registered domain name and obtain information about the owner of a particular website; popular sites of this type include Better-Whois and VeriSign Global Registry Services); SamSpade.org (This site helps officers monitor the activities of offenders who have their own websites. The site provides "ping" WHOIS, trace route information and shows how to use this information, and also the information needed to find the owner of the website and the site's location); Anonymizer (application allows officers to visit offender Websites anonymously without having any unwanted files or code placed on the offenders' computer and without revealing the officer's IP address. This application serves primarily as a deterrent by creating the fear that the officer could be watching at any time). Relevant forensic tools (full description outside scope of article) include EnCase, ComputerCop Professional P3, ComputerCop Forensic and ilook Investigator.

### b. *"Model" Solution I: "Internal" Management Forensics*

Internal Management Forensics, or IMF, involves forensic examinations performed directly by government actors (probation officer or official) as part of the offenders" probation/supervised release. Information gathered through IMF is immediately in the hands of the probation department.

### c. *"Model" Solution II: "External" Management Forensics*

A second proposed solution or model is what I will refer to as "External Management Forensics" (EMF). EMF is conducted by a private forensic examiner not directly employed by the government and is part of the offender's treatment program. EMF has several advantages and follows a strict protocol. As such, the information gathered through EMF is not reported directly to probation officials. Instead, it is reported directly to authorities of the treatment program in which the offender is enrolled (Tx).

The advantages are that EMF: (1) can be accomplished in about 90 minutes; (2) works "live" on the offender's computer; (3) works within the offender's environment; (4) captures approximately 85% of what full computer-forensics captures; and (5) if done properly, is strongly supported by the courts.

*EMF is a five step process*:

1. Written permission is obtained from the offender;[249]

---

[248] The primary differences between Type II "System Resident" and "Forced Gateway" are inherent to the software itself. The two classifications are very similar in result.

[249] The offender pays for the "monitoring" as part of a larger treatment model.

> 2. Examine offender's computer for historical use—the goal is to gain information for the offender's treatment (Tx) team;
> 3. "Sniff" system for keyloggers and look for relevant hardware installed on offender's computer;
> 4. Install monitoring software and set parameters in accordance with case information and previous findings; and
> 5. Wipe free and slack space—this increases the chance of proving a future violation.

### *d. "Model" Solution III: "Hybrid" Management Forensics*

The third "model" solution is a hybrid between models I & II. The monitoring is directly conducted by probation officials as in model I; however, a private company provides monitoring "controls, report generation, server maintenance and data management."[250] The best example of this model is Internet Probation and Parole, Inc. (IPPC) through their service, Impulse ControlTM:

> Impulse ControlTM offers remote monitoring technology, specifically, data is not saved to the offenders system requiring onsite retrieval, rather it is sent in real-time to a controlled environment for review. Officers can easily and conveniently view activity 24/7 remotely. Specialized reports are generated weekly by IPPC and forwarded to members of the supervision team.[251]

---

[250] Internet Probation & Parole Control, Inc. (IPPC) Services Brochure, http://www.impulsecontrol.net (last visited Mar. 29, 2005).

[251] *Id.* (the monitoring covers: Websites visited, files transferred, inbound and outbound communications, Instant messengers, newsgroups/chats, and offline activity and includes keyword restrictions, Internet medium controls, time control restrictions and 24/7 remote access.).

Four Basic Approaches to Management Software:

| TYPE | MAJOR BRAND | ADVANTAGES | DISADVANTAGES |
|---|---|---|---|
| Filtering Software | Cyber Sentinel® | Blocks access to certain sites and logs offender's usage. | |
| System Resident Type I | Spector Pro®<br>True Active® | Spector Pro® is a screen-screen-recording program. It is installed on a drive and configured to 'capture' screen images; it can store up to 5 or 6 days of activity.<br>Spector Pro® works on Windows® and Mac®. | Must be physically present at offender's computer to review usage, etc. Cannot be reviewed remotely. |
| System Resident Type II | E-Blaster® (accompanaies Spector Pro®) | The software e-mails usage reports to Official.<br>Physical presence at computer is not necessary. | Use of system II creates certain time-limitations on the monitoring official—information must be retrieved frequently or the file may become too large and delete 'old' information. The information is actually stored on the offender's drive and therefore can be susceptible to alteration/deletion.<br>Unlike Spector Pro® which works on Windows® and Mac®, E-Blaster® only works on Windows® applications. |

## PART X. RELEVANT BACKGROUND CASELAW

The relevant "split" in the opinions of the various federal appellate circuits is primarily related to a "special restriction" imposed on certain individuals on probation related to either an outright ban on access to the Internet or the requirement that they receive prior permission from a probation officer before doing so.

It is important to remember that the "split" detailed in this section does not involve cases addressing the monitoring of an individual's Internet activity; but, instead involves whether a particular probationer can access the Internet at all or under severely restrictive terms.[252] Although certain aspects of the following cases contain consistencies, due to the distinct sets of facts, a review of the entire line of cases becomes necessary to provide adequate background.[253]

---

[252] This line of cases also primarily deals with whether the "special restriction" at issue is reasonable and thus enforceable under the applicable federal statute and will not directly involve Fourth Amendment analysis.

[253] The following section details cases that are representative of the "split" on this issue currently in the federal circuit courts. *See, e.g.,* United States v. Cabot, 325 F.3d 384 (2d Cir. 2003) (condition of offender's supervised release prohibiting Internet access or other similar computer networks without prior approval from probation officer constituted greater deprivation on offender's liberty than was reasonably necessary); United States v. Fields, 324 F.3d 1025 (8th Cir. 2003) (offender previously convicted of operating child porn website and distributing child porn. Special condition of supervised release prohibited offender from owning or operating any photographic equipment, including computers, scanners, and printers and from having Internet access at his home. Offender also prohibited from owning a computer without prior approval from probation authorities. Special condition upheld as reasonably related to statutory objectives of supervised release); United States v. Freeman, 316 F.3d 386 (3d Cir. 2003) (special condition of supervised release prohibiting offender, convicted of receipt and possession of child pornography, from using or possessing a computer or accessing the Internet without prior (written) approval from the probation department was overly broad and involved a greater deprivation of liberty than reasonably necessary to deter future criminal conduct and protect the public); United States v. Harding, 57 F. App'x 506 (3d Cir. 2003) (computer restriction condition upheld during period of supervised release because condition imposed to deter future criminal conduct and protect the public); United States v. Holm, 326 F.3d 872 (7th Cir.) (supervised release condition banning offender for Internet access held to be a greater deprivation of liberty to serve goals of supervised release), *cert. denied*, 540 U.S. 894 (2003); United States v. Rearden, 349 F.3d 608 (9th Cir. 2003) (condition of supervised release that offender not possess or use a computer with Internet access without prior approval from his probation officer upheld as condition was not absolute and did not plainly [plain error standard] involve greater deprivation of liberty than was reasonably necessary for its purpose), *cert. denied*, 125 S. Ct. 32 (2004); United States v. Ristine, 335 F.3d 692 (8th Cir. 2003) (district court did not commit plain error in restricting offender's use of a computer and Internet

### *United States v. Crandon*[254]

In *Crandon*, the Third Circuit addressed Crandon's challenge to the district court's decision to limit his Internet access during his term of supervised release.[255] Crandon had been previously convicted of one count of receiving child pornography.[256] He was prohibited from any access to the Internet unless it was specifically approved by the U.S. Probation Office.[257] As such, the restriction was broad but did not amount to an outright ban.[258]

The court upheld the broad restriction and held that it was "narrowly tailored" and "reasonably related" to "Crandon's criminal activities."[259] The court, in reviewing the district court's ruling for abuse of discretion, weighed the validity of the condition of supervised release according to 18 U.S.C.

---

access as condition of supervised release); United States v. Taylor, 338 F.3d 1280 (11th Cir.) (special condition on offender's supervised release prohibiting him from using or possessing a computer with Internet access was not unreasonable or overbroad given the underlying conviction), *cert. denied*, 540 U.S. 1066 (2003); United States v. Zinn, 321 F.3d 1084 (11th Cir.) (limited restriction on sex offender's Internet usage while on supervised release was reasonably related to legitimate sentencing considerations and did not overly burden offender's First Amendment rights), *cert. denied*, 540 U.S. 839 (2003); United States v. Walser, 275 F.3d 981 (10th Cir. 2001) (district court did not commit plain error in imposing a special condition of supervised release barring offender from using the Internet without prior approval). For an example of relevant state cases, see *M.G. v. Travis*, 667 N.Y.S.2d 11 (N.Y. App. Div. 1997); Smith v. State, 779 N.E.2d 111 (Ind. Ct. App. 2002); State v. Combs, 10 P.3d 1101 (Wash. Ct. App. 2000); State v. Wardle, 53 P.3d 1227 (Idaho Ct. App. 2002).

[254] 173 F.3d 122 (3d Cir. 1999).

[255] *Id.* at 127 ("The defendant shall not possess, procure, purchase or otherwise obtain access to any form of computer network, bulletin board, Internet, or exchange format involving computers unless specifically approved by the U.S. Probation Office.").

[256] *Id.* at 125. Crandon, a thirty-nine year-old resident of New Jersey, met a fourteen year-old girl over the Internet and traveled to Minnesota to meet her. *Id.* While in Minnesota, Crandon engaged in sexual relations with the minor and took approximately forty-eight pictures of her. *Id.* Two of the photos taken during the three-day trip were sexually explicit; one showed Crandon and the girl engaged in oral sex. *Id.*

[257] *Id.*

[258] *Id.* at 127-28.

[259] *Id.*

§ 3583.[260]

Pursuant to 18 U.S.C. § 3583, a district court may order any appropriate condition to the extent that it:

> (1) is reasonably related to certain factors, including:
>     (a) the nature and circumstances of the offense and the history and characteristics of the defendant;
>     (b) deterring further criminal conduct by the defendant; or
>     (c) protecting the public from further criminal conduct by the defendant; and
>
> (2) involves no greater deprivation of liberty than is reasonably necessary for the purposes of deterrence and protection of the public.[261]

### *United States v. White*[262]

In *United States v. White*, the Tenth Circuit addressed a probationer's challenge to the restriction that he "'shall not possess a computer with Internet access throughout his period of supervised release.'"[263] White had previously been convicted of receiving child pornography.[264]

The court was critical of the wording of this restriction and found that it did not appear to meet its intended goal:

> As worded, the prohibition does not bar Mr. White's access to

---

[260] *Id.* at 127 ("The validity of a condition of supervised release is governed by 18 U.S.C. § 3583."). The court expressly noted that in this context, the "abuse of discretion" standard was even more relaxed within the context of probation. *Id.* at 128. "We believe that the District Court carefully considered Crandon's prior conduct and the need to protect the public and did not abuse its *broad discretion* when it prohibited Crandon from accessing the Internet or other similar computer networks without prior approval . . . ." *Id.* (emphasis added).

[261] *Id. See also* 18 U.S.C. §§ 3583(d), 3553(a) (2000).

[262] 244 F.3d 1199 (10th Cir. 2001).

[263] *Id.* at 1205.

[264] *Id.* at 1201. In 1996, White (using the e-mail address Lech23@aol.com) responded to an advertisement placed by United States Customs officers and placed an order for three videos of young girls engaged in fondling and sexual intercourse with adult men. *Id.* White was arrested after taking delivery of the videos. *Id.*

> the Internet; only his possession of a computer with Internet access. The distinction is not without a difference. Despite the apparent constraint, Mr. White may visit a library, cybercafe, even an airport, and log onto the Internet. The Internet is also accessible *via* web-t.v. by attaching an electronic device to a television. Consequently, if the district court targeted this special condition at the nature and circumstances of the offense and Mr. White's history and characteristics to prevent using the Internet to order child pornography, it missed the mark.[265]

The court held that if the district court intended an outright ban on Internet access by equating the term "possess" with any Internet access or use at all, then the restriction was overreaching and "greater than necessary" under the federal statute.[266] The court reasons that if this were the case the probationer would not be able to use "a computer at a library to do any research, get a weather forecast, or read a newspaper online."[267]

As expected, the court in *White* appears to disfavor any special restriction that imposes an outright ban on Internet access, especially given the increasing role the Internet plays in American life.[268] The court's analogy of the Internet to a telephone indicates that, at least in certain courts, access to the Internet will be deemed a modern necessity.

The court also indicates that, due to the vastness of the Internet generally, and the manner in which it can be easily accessed, an outright ban is not only legally problematic but also realistically unenforceable:

> [The Internet's] instant link to information is akin to opening

---

[265] *Id.* at 1205. The court noted in a footnote that there was some question as to exactly when a computer has Internet access. *Id.* at 1205 n.7.

[266] *Id.* at 1206 ("Under these circumstances, the special condition is "greater than necessary," 18 U.S.C. § 3553(a), and fails to balance the competing interests the sentencing court must consider.").

[267] *Id.*

[268] *Id.* at 1207 ("Given the openness of cyberspace, if the court instead chooses to prohibit [probationer from] using any computer, we must caution against this broad sweep . . . .").

> a book. Indeed cyberspace defies boundaries; it offers unlimited access. "[T]he openness of this architecture means this: That there is no 'natural' or simple or 'automatic' way to keep people out because there are no natural or real borders that close off access to those who should not have access."[269]

The court held that the special condition was "neither reasoned nor reasonable" and remanded the case to the district court to define exactly what is meant by "possession of a computer with access to the Internet . . . ."[270]

### *United States v. Peterson*[271]

In *United States v. Peterson*, the Second Circuit held that an outright ban that "prohibit[s] the defendant outright from possessing or using a computer that includes either a modem, an Internet account, a mass storage device, or a writable or rewritable CD Rom"[272] was not "reasonably related" to "the nature and circumstances of the offense" or probationer's "history and characteristics."[273]

The district court imposed the computer and Internet restrictions not based on the underlying crime of bank larceny, but instead, on an earlier conviction for incest.[274] The court expressly noted that "[t]here is no indication that Peterson's past incest offense had any connection to computers or to the Internet."[275] Given the lack of a relationship between the underlying sexual offense (incest) and computers or the Internet, the court held that the necessary standard of "reasonably related" had not been met.[276]

---

[269] *Id.* (citing Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 Emory L.J. 869, 887 (1996)).

[270] *Id.* at 1207.

[271] 248 F.3d 79 (2d Cir. 2001).

[272] *Id.* at 82-83.

[273] *Id.* (citing 18 U.S.C. §§ 3563(b) & 3553). *See also* 18 U.S.C. §§ 3553(a)(2), 3563(b) (2000).

[274] *Peterson*, 248 F.3d at 82-83.

[275] *Id.* at 83.

[276] *Id.* ("Nor is the ban on computer or Internet use reasonably necessary to protect the public or Peterson's family from future crimes, or to any of the nu-

The Second Circuit followed the Tenth Circuit's lead in *White* and re-emphasized the "virtually indispensable" nature of Internet access in modern life: "Computers and Internet access have become virtually indispensable in the modern world of communications and information gathering. The fact that a computer with Internet access offers the possibility of abusive use for illegitimate purposes does not, at least in this case, justify so broad a prohibition."[277]

Had the Second Circuit affirmed the lower court's restriction, holding that the previous crime of incest was sufficient to allow for an outright ban, a rule might emerge (at least in the Second Circuit) that *any* sexual offense would pave the way for a special restriction banning Internet access. In *Peterson*, it appears that even a serious sexual offense (like incest) has to have been committed in such a way that links the criminal activity to access to the Internet.[278] The court appears to leave open, by distinguishing the case through the use of the phrase "in this case," that it may not continue, in all circumstances, to adhere to the *per se* rule established in *White*.[279] Instead, the Second Circuit leaves open the possibility that in certain cases an outright Internet ban may be allowable based on the relationship between the underlying sexual offense and Internet access.[280]

### *United States v. Paul*[281]

In *United States v. Paul*, the Fifth Circuit addressed the following broad probation restriction: "[Paul] . . . . 'shall not have [,] possess or have access to computers, the Internet, photographic equipment, audio/video equipment, or any item capa-

---

merous broad sentencing grounds set forth in § 3553(a)(2).").

[277] *Id.* (citing United States v. White, 244 F.3d 1199, 1206 (10th Cir. 2001)). This is the portion of the *White* opinion that the Fifth Circuit rejects in *United States v. Paul*, 274 F.3d 155, 169 (5th Cir. 2001).

[278] *Peterson*, 248 F.3d at 83.

[279] *Id.*

[280] *Id.* at 83-84.

[281] 274 F.3d 155 (5th Cir. 2001).

ble of producing a visual image.'"[282]

Paul pled guilty to one charge of "knowingly possessing a computer hard drive with three or more images of child pornography that traveled in interstate commerce . . . ."[283] Paul also had a previous 1986 conviction involving child pornography and, at the time his residence was searched, also possessed assorted materials related to child pornography, a large bag of children's clothes, and several children's swimsuits covered with sand.[284] Further, a review of Paul's computer revealed e-mail messages that discussed "sources of child pornography, including websites, chat rooms, and newsgroups that allowed both receiving and sending pornographic images."[285] One particularly disturbing e-mail discussed "how easy it was to find 'young friends' by scouting single, dysfunctional parents through Alcoholics Anonymous or local welfare offices and winning their friendship, thereby securing access to their young sons."[286]

Paul appealed the special restriction contending that a "blanket prohibition on computer or Internet use is excessively broad" and could not be justified solely on the fact that his underlying crime involved a computer and the Internet.[287] The court, noting that Paul's computer contained over 1200 images of child pornography and evidence that Paul had used the Internet to "'scout' single, dysfunctional parents and gain access to their children," upheld the restriction and held that the district court had not abused its discretion in imposing it.[288]

---

[282] *Id.* at 160.

[283] *Id.* at 158.

[284] *Id.* ("Additionally, the agents seized a medical bag containing basic medical supplies and Spanish-language flyers advertising lice removal for children. In the flyers, Paul informed parents that he would spray their children with a product that kills lice. The flyers also stated that Paul would conduct a complete physical examination on each child for 'overall health,' which necessarily required the child to completely undress.").

[285] *Id.*

[286] *Id.*

[287] *Id.* at 168.

[288] *Id.* at 168-70.

The court, citing *Crandon*, held that given the underlying facts the special restriction in both cases was "reasonably related to [probationer's] offense and to the need to prevent recidivism and protect the public."[289] The court acknowledged that the special restriction in *Paul* was broader than the one at issue in *Crandon* because "it contains no proviso permitting Paul to use these resources with the approval of his probation office."[290]

---

[289] *Id.* at 169. "The record reveals that Paul has in the past used the Internet to encourage exploitation of children by seeking out fellow 'boy lovers' and providing them with advice on how to find and obtain access to 'young friends.'" *Id.* The court, in addition to citing *Crandon* as an example of courts that had upheld Internet and computer restrictions as conditions of supervised release, also cited *United States v. Mitnick*, 145 F.3d 1342 (9th Cir. 1998) (unpublished table decision). In *Mitnick*, the Ninth Circuit "reject[ed] [probationer's] specific contention that the supervised release conditions impermissibly restrict the exercise of his First Amendment rights. *Mitnick*, 145 F.3d at 1342 (citing United States v. Bolinger, 940 F.2d 478, 480-81 (9th Cir. 1991)). *Bolinger* upheld a probation condition which restricted defendant's freedom of association. The court in *Paul* also distinguished the Second Circuit's opinion in *United States v. Peterson*, 248 F.3d 79, 81-83 (2d Cir. 2001). *Paul*, 274 F.3d at 168 n.15. The distinction in *Peterson* involved special conditions involving computer and Internet access that were actually related to a previous sex offense and not the applicable underlying charge of bank larceny. *Id.*

[290] *Paul*, 274 F.3d at 169; *see also* United States v. Fields, 324 F.3d 1025 (8th Cir. 2003). In *Fields*, the Eighth Circuit upheld extremely restrictive terms of supervised release related to Internet access and computer use. *Fields*, 324 F.3d at 1027. The court expressly stated that the conditions did not amount to an outright ban because "[H]e may use and even possess a computer with the permission of his probation officer." *Id.* The court distinguished the Second Circuit's ruling in *Sofsky* which involved "simple possession of child pornography" and cited to cases where more significant exploitation of children was found. *Id.* The court found the obvious, the that Fields's crime involved more than simple possession of child pornography. *Id.* "In the summer of 2001 Fields created lolitgurls.com, an internet [sic] site that provided subscribers access to 'hard to find' and 'shocking' nude pictures of 'girls age 12-17.'" *Id.* at 1026. Three months later, the Eighth Circuit ruled similarly in *United States v. Ristine*, 335 F.3d 692 (8th Cir. 2003). Holding that the exploitation of young girls in Ristine's crime was "of the same degree" as Fields's crime, the court upheld the restrictive terms of supervised release. *Ristine*, 335 F.3d at 696. Another similarity in both cases is that neither defendant objected to the terms of supervised release of sentencing and therefore the court would review the terms of release for "plain error" instead of "abuse of discretion." *Fields*, 324 F.3d at 1026; *Ristine*, 335 F.3d at 694. It is unclear whether the court would have ruled differently if reviewing the terms for "abuse of discretion." The court hinted that it might make a difference under certain

The Fifth Circuit expressly rejected the Tenth Circuit's reasoning in *White*, "that an absolute prohibition on accessing computers or the Internet is per se an unacceptable condition of supervised release, simply because such a prohibition might prevent a defendant from using a computer at the library to 'get a weather forecast' or to 'read a newspaper online.'"[291]

In *United States v. Sofsky*, the Second Circuit, expressly noting its earlier ruling in *Peterson*,[292] held that:

> Although the condition prohibiting Sofsky from accessing a computer or the Internet without his probation officer's approval is reasonably related to the purposes of his sentencing, in light of the nature of his offense, we hold that the condition inflicts a greater deprivation of privacy on Sofsky's liberty than is reasonably necessary.[293]

*Sofsky* also serves as a transitional case. While re-affirming the Second Circuit's general holding in *Peterson*, its ruling is somewhat confusing when read in conjunction with the Second Circuit's ruling in *United States v. Lifshitz* two years later.[294]

*Sofsky* seems to explicitly endorse computer monitoring because it provides a less-restrictive means of monitoring computer use and Internet access than banning access altogether or with prior governmental permission.

> The Government contended at oral argument that the [computer use/monitoring] restriction must be broad because a restriction limited to accessing pornography would be ex-

---

circumstances, "[w]ere we reviewing this special condition for an abuse of discretion, we might be forced to select the line of reasoning we find more compelling, but the standard here is plain error." *Ristine*, 335 F.3d at 695.

[291] *Paul*, 274 F.3d at 169-70.

[292] *Sofsky*, 287 F.3d at 126 ("We previously considered a sentencing component that prohibited access to a computer or the Internet in *United States v. Peterson*, 248 F.3d 79, 82-83 (2d Cir. 2001)).

[293] *Id.*

[294] 369 F.3d 173 (2d Cir. 2002).

> tremely difficult for the probation officer to enforce without constant monitoring of Sofsky's use of his computer. There are several responses. First, to the extent that even a broad restriction would be enforced by the probation officer, monitoring (presumably unannounced) of Sofsky would be required to check if he was using a computer at all. Second, a more focused restriction, limited to pornography sites and images, *can be enforced by unannounced inspections of Sofsky's premises and examination of material stored on his hard drive or removable disks.*[295]

The court continued in Footnote 4, "[o]ne of the standard conditions of supervised release imposed on Sofsky requires him to 'permit a probation officer to visit him . . . at any time at home or elsewhere.'"[296]

## CONCLUSION

How the Fourth Amendment acts to limit the actions of government actors who want to search and/or monitor the computers of probationers with a conviction for Internet-related child pornography may come down to footnotes. While footnote 15 in *Ferguson* and footnote 6 in *Knights* will not likely rise to the prominence of footnote 4 in *United States v. Carolene Products Co.*,[297] for our purposes they are the best indicators to answer the question: *what next?*

The "special needs" doctrine is a totally incoherent doctrine that is not driven by "special needs" but instead by "special interests,"[298] that allows the reviewing court to act as a "policy Magistrate."[299]

---

[295] *Sofsky*, 287 F.3d at 126-27 (emphasis added).

[296] *Id.* at 127. It seems that the Second Circuit held that there were less restrictive means to accomplish the legitimate policy aims of probation (*Peterson*, *Sofsky*) but then also struck down the express 'less-restrictive mean[s]' of monitoring instead of the outright Internet-access ban (*Lifshitz*).

[297] *See* United States v. Carolene Prods. Co., 304 U.S. 144, 153 n.4 (1938) (Justice Stone's famous footnote referring to "discrete and insular minorities").

[298] *See supra* note 128 and accompanying text.

[299] *See* Sundby, *supra* note 7, at 550-51 ("The question for the future is wheth-

However, given the application of "special needs" by the Second Circuit in *Lifshitz*, (a case dealing specifically with computer monitoring in the probation context) and footnote 15 in *Ferguson*, the "'special needs' of probationers doctrine" continues to appear as the most viable, and most prominent, analysis for the Court to apply when reviewing the 'reasonableness' of a warrantless search in the probationary context. However, if 'special needs' does not get the Court where it wants to go, the more general reasonableness inquiry applied in *Knights* remains as a separate, and potent, alternative for application by a results-oriented judiciary.

With regards to reasonableness as the appropriate inquiry, the possibility remains, albeit unlikely, that the Court will answer the second question left open in *Knights*' footnote 6 and rule that probationers simply have either no "reasonable expectation of privacy" or one so diminished that a warrantless search would be considered *per se* reasonable. If this occurs, similar to a finding of waiver, the Fourth Amendment inquiry would end.

Turning to how this type of warrantless search fits into the larger history, context and jurisprudence of the Fourth Amendment, it appears likely that whatever approach applied by the Court: waiver, reasonableness, or "special needs," will be viewed in light of the new and explosive era of Internet-related crime against children that will likely join the wars on drugs and terror as a type of societal threat able to re-define what is objectively and subjectively "reasonable" within our culture.

To create a hierarchy of the proper analysis between the three, this article proposes that the Seventh Circuit was correct in *Barnett*, in its holding that (valid) waiver alone justifies the warrantless search of a probationer's home, or a computer located in the home, pursuant to the express language of the conditions of probation and, as such, that the United States Supreme Court should follow this reasoning.

That is what the Court should do. However, in the shorter-

---

er the Court will continue in its role as an active 'policy magistrate'. . . .").

term, I believe that the Court's strategy is to constantly create and then interchange doctrines and "balancing tests" so that it can reach any result it favors in the minute fraction of cases it chooses to hear.

In closing, I am pragmatic and join Professor Maclin's opinion that at times the Court creates a "Good for this Day and Train Only theory" to reach its intended results.[300] Although I maintain that the "special needs" analysis will most likely govern this type of search, and guide its relative place in Fourth Amendment jurisprudence, the most recent on-point case is *Knights*, and therefore it cannot be seen as anything but a close second. In *Knights*, the Court turned to a "totality" or "general reasonableness model," a "standardless formula that permits a majority of the Court to do what it pleases without having to justify its results or reasoning under traditional Fourth Amendment doctrine."[301] As this is the case, the Court's future decisions in this area become almost impossible to predict as we are left in the dark as to which test will be applied under any particular set of circumstances.

"Liberty finds no refuge in a jurisprudence of doubt" were the Court Majority's hollow, and intellectually dishonest, opening words in its oft-criticized 1992 decision *Planned Parenthood v. Casey*.[302] Although these words dramatically failed to start the Court on a new road to consistency in 1992,[303] and are nonsensical in the context they were penned, standing alone, they are true.

---

[300] Tracey Maclin, *Is Obtaining an Arrestee's DNA a Valid Special Needs Search Under the Fourth Amendment? What Should (and will) the Supreme Court Do?*, 33 J.L. MED. & ETHICS 102, 118 n.261 (2005).

[301] *Id.*

[302] Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 844 (1992).

[303] *See, e.g.*, Lawrence v. Texas, 539 U.S. 558, 586 (2003) (Scalia, J., dissenting).

> That was the Court's sententious response, barely more than a decade ago, to those seeking to overrule *Roe v. Wade*, 410 U.S. 113 (1973). The Court's response today, to those who have engaged in a 17-year crusade to overrule *Bowers v. Hardwick*, 478 U.S. 186 (1986), is very different. The need for stability and certainty presents no barrier.

*Id.*

The Court needs to focus on eliminating its "jurisprudence of doubt" not only between new cases and precedent they would affect, or overrule, generally, but also within the text of its decisions specifically. The inexplicable and interchangeable use of legal formulae, standardless standards and balancing tests that are not even inherently balanced has led to a "jurisprudence of doubt" at the whim of this Nation's least representative branch of government.[304]

---

[304] *See supra* note 109 and accompanying text.

## APPENDIX I
## Relevant State Statutes

### STATE STATUTES

**California**
CAL. PENAL CODE § 1203.047 (West 2004). Conviction of computer crime; probation

A person convicted of certain enumerated computer crimes may be granted probation, but, . . . [d]uring the period of probation, that person shall not accept employment where that person would use a computer connected by any means to any other computer, except upon approval of the court and notice to and opportunity to be heard by the prosecuting attorney, probation department, prospective employer, and the convicted person. Court approval shall not be given unless the court finds that the proposed employment would not pose a risk to the public.

**Florida**
FLA. STAT. ANN. § 948.03(5)(a)(7) (West 2001). Terms and conditions of probation or community control

(5)(a)(7). Unless otherwise indicated in the treatment plan provided by the sexual offender treatment program, a prohibition on viewing, owning, or possessing any obscene, pornographic, or sexually stimulating visual or auditory material, including telephone, electronic media, computer programs, or computer services that are relevant to the offender's deviant behavior pattern.

**Illinois**
725 ILL. COMP. STAT. ANN. § 207/40(b)(5)(T) (West Supp. 2005). Commitment

(b)(5) An order for conditional release places the person in the custody, care, and control of the Department. The court shall order the person be subject to the following rules of conditional release, in addition to any other conditions ordered, and the person shall be given a certificate setting forth the conditions of conditional release. These conditions shall be that the person:
(T) neither possess or have under his or her control any material

that is pornographic, sexually oriented, or sexually stimulating, or that depicts or alludes to sexual activity or depicts minors under the age of 18, including but not limited to visual, auditory, telephonic, electronic media, or any matter obtained through access to any computer or material linked to computer access use.

**Minnesota**
MINN. STAT. ANN. § 243.055 (West 2003). Computer Restrictions

Subdivision 1. Restrictions to use of online services. If the commissioner believes a significant risk exists that a parolee, state-supervised probationer, or individual on supervised release may use an Internet service or online service to engage in criminal activity or to associate with individuals who are likely to encourage the individual to engage in criminal activity, the commissioner may impose one or more of the following conditions:
(1) prohibit the individual from possessing or using a computer with access to an Internet service or online service without the prior written approval of the commissioner;
(2) prohibit the individual from possessing or using any data encryption technique or program;
(3) require the individual to consent to periodic unannounced examinations of the individual's computer equipment by a parole or probation agent, including the retrieval and copying of all data from the computer and any internal or external peripherals and removal of such equipment to conduct a more thorough inspection;
(4) require consent of the individual to have installed on the individual's computer, at the individual's expense, one or more hardware or software systems to monitor computer use; and
(5) any other restrictions the commissioner deems necessary.
Subd. 2. Restrictions on computer use. If the commissioner believes a significant risk exists that a parolee, state-supervised probationer, or individual on supervised release may use a computer to engage in criminal activity or to associate with individuals who are likely to encourage the individual to engage in criminal activity, the commissioner may impose one or more of the following restrictions:
(1) prohibit the individual from accessing through a computer any material, information, or data that relates to the activity involved in the offense for which the individual is on probation, parole, or supervised release;

(2) require the individual to maintain a daily log of all addresses the individual accesses through computer other than for authorized employment and to make this log available to the individual's parole or probation agent;
(3) provide all personal and business telephone records to the individual's parole or probation agent upon request, including written authorization allowing the agent to request a record of all of the individual's outgoing and incoming telephone calls from any telephone service provider;
(4) prohibit the individual from possessing or using a computer that contains an internal modem and from possessing or using an external modem without the prior written consent of the commissioner;
(5) prohibit the individual from possessing or using any computer, except that the individual may, with the prior approval of the individual's parole or probation agent, use a computer in connection with authorized employment;
(6) require the individual to consent to disclosure of the computer-related restrictions that the commissioner has imposed to any employer or potential employer; and
(7) any other restrictions the commissioner deems necessary.
Subd. 3. Limits on restriction. In imposing restrictions, the commissioner shall take into account that computers are used for numerous, legitimate purposes and that, in imposing restrictions, the least restrictive condition appropriate to the individual shall be used.

**Nevada**
NEV. REV. STAT. ANN. § 176A.413 (LexisNexis Supp. 2001). Restrictions relating to computers and use of Internet and other electronic means of communication; powers and duties of court; exceptions.

1. Except as otherwise provided in subsection 2, if a defendant is convicted of stalking with the use of an Internet or network site or electronic mail or any other similar means of communication pursuant to subsection 3 of NRS 200.575, an offense involving pornography and a minor pursuant to NRS 200.710 to 200.730, inclusive, or luring a child or mentally ill person through the use of a computer, system or network pursuant to paragraph (a) or (b) of subsection 4 of NRS 201.560 and the court grants probation or suspends the sentence, the court shall, in addition to any other condition ordered pursuant to NRS 176A.400, order as a condition of probation or suspension that the defendant not own or use a computer, including,

without limitation, use electronic mail, a chat room or the Internet.
2. The court is not required to impose a condition of probation or suspension of sentence set forth in subsection 1 if the court finds that:
(a) The use of a computer by the defendant will assist a law enforcement agency or officer in a criminal investigation;
(b) The defendant will use the computer to provide technological training concerning technology of which the defendant has a unique knowledge; or
(c) The use of the computer by the defendant will assist companies that require the use of the specific technological knowledge of the defendant that is unique and is otherwise unavailable to the company.
3. Except as otherwise provided in subsection 1, if a defendant is convicted of an offense that involved the use of a computer, system or network and the court grants probation or suspends the sentence, the court may, in addition to any other condition ordered pursuant to NRS 176A.400, order as a condition of probation or suspension that the defendant not own or use a computer, including, without limitation, use electronic mail, a chat room or the Internet.
4. As used in this section:
(a) "Computer" has the meaning ascribed to it in NRS 205.4735.
(b) "Network" has the meaning ascribed to it in NRS 205.4745.
(c) "System" has the meaning ascribed to it in NRS 205. 476.

NEV. REV. STAT. ANN. § 213.1258 (LexisNexis 2005). Conditions relating to computers and use of Internet and other electronic means of communication; powers and duties of board; exceptions.

1. Except as otherwise provided in subsection 2, if the Board releases on parole a prisoner convicted of stalking with the use of an Internet or network site or electronic mail or any other similar means of communication pursuant to subsection 3 of NRS 200.575, an offense involving pornography and a minor pursuant to NRS 200.710 to 200.730, inclusive, or luring a child or mentally ill person through the use of a computer, system or network pursuant to paragraph (a) or (b) of subsection 4 of NRS 201.560, the Board shall, in addition to any other condition of parole, require as a condition of parole that the parolee not own or use a computer, including, without limitation, use electronic mail, a chat room or the Internet.
2. The Board is not required to impose a condition of parole set forth

in subsection 1 if the Board finds that:
(a) The use of a computer by the parolee will assist a law enforcement agency or officer in a criminal investigation;
(b) The parolee will use the computer to provide technological training concerning technology of which the defendant has a unique knowledge; or
(c) The use of the computer by the parolee will assist companies that require the use of the specific technological knowledge of the parolee that is unique and is otherwise unavailable to the company.
3. Except as otherwise provided in subsection 1, if the Board releases on parole a prisoner convicted of an offense that involved the use of a computer, system or network, the Board may, in addition to any other condition of parole, require as a condition of parole that the parolee not own or use a computer, including, without limitation, use electronic mail, a chat room or the Internet.
4. As used in this section:
(a) "Computer" has the meaning ascribed to it in NRS 205.4735.
(b) "Network" has the meaning ascribed to it in NRS 205.4745.
(c) "System" has the meaning ascribed to it in NRS 205. 476.

**North Dakota**
N.D. CENT. CODE § 12.1-32-07(4)(r) (Supp. 2005). Supervision of probationer—Conditions of probation—Revocation.

4. When imposing a sentence to probation, probation in conjunction with imprisonment, or probation in conjunction with suspended execution or deferred imposition of sentence, the court may impose such conditions as it deems appropriate and may include any one or more of the following: r. Refrain from any subscription to, access to, or use of the Internet.

## General Statutory Overview Warrantless Searches Pursuant to Probation or Parole (Not necessarily related to Computer Monitoring)

### State Statutes

| | |
|---|---|
| Alaska | Alaska Stat. § 33.16.150(b)(3) |
| California | Cal. Penal Code § 3067(a) |
| Colorado | Colo. Rev. Stat. §17-2-201(5)(f)(I)(D) |
| Florida | Fla. Stat. Ann. § 48.03(1)(5)(a)(10) |
| Illinois | 730 Ill. Comp. Stat. § 5/3-3-7(a)(10) |
| Indiana | Ind. Code § 11-13-3-7 (7)(a)(6) |
| Maine | Me. Rev. Stat. Ann. tit. 17-A, § 1264(2)(C) |
| Nevada | Nev. Rev. Stat. § 4.373(1)(g) |
| New York | N.Y. Crim Proc. Law § 410.50 |
| North Carolina | N.C. Gen. Stat. § 15A-1343(b1)(7)<br>N.C. Gen. Stat. § 15A-1374(b)(11) |
| North Dakota | N.D. Cent. Code § 12.1-32-07(4)(n) |
| Ohio | Ohio Rev. Code Ann. § 2951.02<br>Ohio Rev. Code Ann. § 2967.131(C)<br>Ohio Rev. Code Ann. § 2971.07(C) |
| Oregon | Or. Rev. Stat. § 137.540(1)(i)<br>Or. Rev. Stat. § 144.102(3)(b)(H) |
| Pennsylvania | 61 Pa. Cons. Stat. Ann. § 331.27a<br>61 Pa. Const. Stat. Ann. § 331.27b |
| Rhode Island | R.I. Gen. Laws § 42-56-20.2(d)(1)(2) |

**Administrative Code**

| | |
|---|---|
| Michigan | Mich. Admin. Code R. 791.77.35 |

**Court Rules**

| | |
|---|---|
| New Hampshire | N.H. Super. Ct. R. 107<br>N.H. Dist. & Mun. Ct. R. 2.17 |

# ADVERTISING IN THE MISSISSIPPI LAW JOURNAL

If you are interested in purchasing this available advertising space, please call Peggy Nail at 662-915-6870 or e-mail her *at* pnail@olemiss.edu to inform us of your interest. Upon request, the Mississippi Law Journal can provide potential advertisers with a list of advertising prices, as well as help with any questions that they may have about advertising in the Mississippi Law Journal.

**BROOKS COURT REPORTING**

P.O. Box 2632 ■ Jackson, MS 39207
Phone: (601) 362-1995 ■ Fax: (601) 362-2445
www.BrooksReporting.com

# National Center for Justice and the Rule of Law

*The University of Mississippi School of Law*

The National Center for Justice and the Rule of Law is a part of the University of Mississippi School of Law. The Center focuses on issues relating to the criminal justice system, with its purpose to promote the two concepts comprising the title of the Center. The concept of "justice" appeals to basic notions of equality, equity, and fairness, often with an emotive component. In contrast, the phrase "rule of law" refers to the requirement that certain procedures and principles must be followed in each case to reach a correct result. Neither concept is sufficient; rather, both must be utilized to ensure that the criminal justice system fulfills its function in society. The Center implements its mission through projects, conferences, educational programs, and publications that examine important criminal law and procedural issues.

Thomas K. Clancy
Director

The Center has five programs:

***National Programs Initiative***

Helps state governments investigate sophisticated criminal activity through training and model programs designed to attack computer-related crime.

***Fourth Amendment Initiative***

Promotes awareness of search and seizure principles through conferences, training, and support for selected publications.

***Prosecution Externship Program***

Provides specialized course-work and real-world training for law students in the duties and responsibilities of prosecutors.

***Criminal Appeals Clinic***

Provides law students with intensive training representing on appeal persons convicted of crimes.

***Special Projects***

Provides support for selected projects that promote the concepts of justice and the rule of law.

Visit the Center's website at www.NCJRL.org for additional information about these programs.